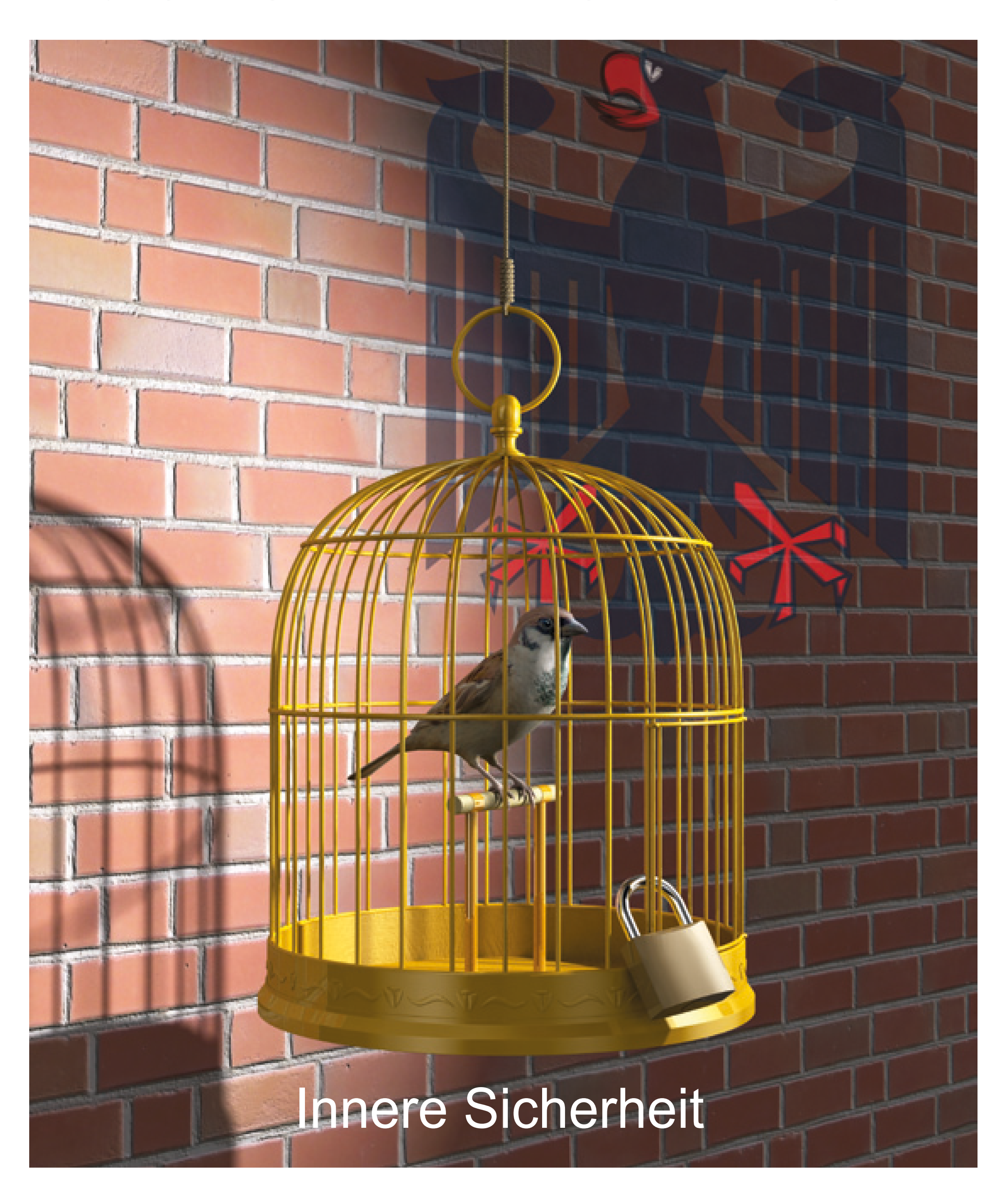
1/2016

Datenschutz Nachrichten

39. Jahrgang
ISSN 0137-7767
12,00 Euro

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de



■ Transatlantische Sicherheitskooperation und Datenschutz – Was bringt das „Umbrella Agreement"? ■ Die EU-Richtlinie für den Datenschutz bei Polizei und Justiz ■ PERSONAL DATA NOT FOUND: Personenbezogene Entscheidungen als überfällige Neuausrichtung im Datenschutz ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Inhalt



Termine

Freitag, 22. April 2016
Big Brother Awards
Bielefeld, Hechelei
https://bigbrotherawards.de/

Samstag, 23. April 2016
DVD-Vorstandssitzung
Bielefeld. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Sonntag, 18. September 2016
DVD-Vorstandssitzung
Kiel. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Montag, 19. September 2016
ULD-Sommerakademie
Kiel
https://www.datenschutzzentrum.de/sommerakademie/

Samstag, 22. Oktober 2016
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Sonntag, 23. Oktober 2016
DVD-Mitgliederversammlung
Bonn.
dvd@datenschutzverein.de

Foto: Uwe Schlick / pixelio.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
39. Jahrgang, Heft 1

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Thilo Weichert
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße. 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@t-online.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0)91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta

Editorial

Liebe Leserinnen und Leser,

während fast alle über Syrien und die Flüchtlingskrise diskutieren, werden für die Infrastruktur und normativen Grundlagen unseres digitalisierten Informationsverhaltens Festlegungen vorgenommen. Dies beginnt mit der digitalen Erfassung der Flüchtlingsströme, von den Fingerabdrücken bis hin zur Speicherung von Religion und Ethnizität – für uns in Mitteleuropa ein Ding diskriminierungsträchtiger Unmöglichkeit, für die konfliktreduzierende Verwaltung von Flucht aber (fast) eine Notwendigkeit. Die DANA wird auf dieses Thema zurückkommen, zumal es Rückwirkungen darauf hat, wie wir generell mit Digitalem umgehen.

Im Windschatten ist aber – fast – die Europäische Grundverordnung (EU-DSGVO) aus dem Blickfeld verschwunden. Der dazu im Trilog kurz vor Weihnachten 2015 gefundene Kompromiss wird uns noch viele Jahre beschäftigen, die DANA 2/2016 wird sich damit vertieft befassen. Wer hierzu Kluges, Neues und Hintergründiges zu bieten hat, auch gerne zu Einzelaspekten, ist herzlich eingeladen, bis zum Redaktionsschluss dieses Heftes am 1. Mai Beiträge einzureichen.

Während die EU-DSGVO in der Öffentlichkeit zumindest noch wahrgenommen wurde, blieb deren kleine Schwester, die Europäische Datenschutzrichtlinie für Justiz und Polizei, völlig unter dem Radar der Wahrnehmung, selbst von Datenschützerinnen und Datenschützern. Dieser schwarze Fleck soll mit dem vorliegenden Heft etwas aufgehellt werden. Wie wichtig die Wahrung des Datenschutzes in Zeiten eines gesteigerten subjektiven Bedürfnisses nach „innerer Sicherheit" ist, verschwindet insbesondere bei unseren Nachbarn in Europa und auf der anderen Seite des Atlantiks vom Schirm der Wahrnehmung. Deshalb müssen wir uns mit den Bestrebungen in diesen Ländern – u. a. hier in den DANA-Meldungen – befassen, sowie mit den Kooperationsinstrumenten. Zu diesen gehört nicht nur die Richtlinie für Justiz und Polizei, sondern auch das geplante Umbrella-Abkommen mit den USA. Peter Schaar gibt uns hierzu Einblicke, welche uns nicht nur optimistisch stimmen können. Umbrella ist die institutionalisierte andere Seite des neu erfundenen EU-US Privacy Shields, mit dem sich die US-Sicherheitsbehörden weiterhin einen Zugang zu europäischen Datenbeständen sichern wollen.

Der Blick in die nicht immer rosige Realität darf uns nicht davon abhalten, über die Grundlagen unseres praktizierten Datenschutzes nachzudenken, da dies die Voraussetzung dafür ist, diesen zukunftsweisend weiterzuentwickeln. Jörg Pohle liefert hierzu unkonventionelle Gedanken, die nicht nur zum Nachdenken, sondern auch zur Diskussion einladen.

Viel Spaß und viele Erkenntnisse beim Lesen wünscht und auf kluge Reaktionen hofft die gesamte DANA-Redaktion einschließlich

Thilo Weichert

Autorinnen und Autoren dieser Ausgabe:

Jörg Pohle

studierte Rechtswissenschaft, Politikwissenschaft und Informatik. Derzeit promoviert er an der Humboldt-Universität zu Berlin zur Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung und koordiniert am Alexander von Humboldt Institut für Internet und Gesellschaft ein interdisziplinäres Forschungsprojekt zu Fragen der globalen Aushandlung im Privacy- und Datenschutzbereich (http://www.hiig.de/project/privacy-governance/).

Peter Schaar

Ehemaliger Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. psch@eaid-berlin.de

Dr. Thilo Weichert

Ehemaliger Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein, Kiel, Vorstandsmitgied in der DVD, weichert@datenschutzexpertise.de

Peter Schaar

Transatlantische Sicherheitskooperation und Datenschutz – Was bringt das „Umbrella Agreement"?

Die Europäische Kommission verspricht, dass das im Herbst letzten Jahres mit der US-Regierung ausgehandelte Rahmenabkommen zum Datenschutz beim Datenaustausch für Zwecke der Strafverfolgung („Umbrella Agreement") einen angemessenen Schutz der aus der EU in die Vereinigten Staaten übermittelten personenbezogenen Daten garantiert. In dem folgenden Beitrag wird der Hintergrund dieses Abkommens erläutert und es wird der Frage nachgegangen, ob damit tatsächlich das behauptete Schutzniveau erreicht wird.



1. Intensivierter Datenaustausch nach dem 11. September 2001

Die Zusammenarbeit zwischen europäischen und US-amerikanischen Sicherheitsbehörden hat eine lange Geschichte, die bis heute durch die Dominanz der US-Seite geprägt ist, wie etwa die Enthüllungen Edward Snowdens gezeigt haben. Nach den terroristischen Attentaten vom 11. September 2001 strebten die Vereinigten Staaten – als Teil einer umfassenden, vom damaligen Präsidenten G.W. Bush proklamierten Strategie[1] – einen möglichst umfassenden Datenaustausch mit den ausländischen Verbündeten an. Bereits im Dezember 2001 schloss die US-Regierung mit dem Europäischen Polizeiamt Europol ein Abkommen[2] zur intensivierten Kooperation und zum strategischen Informationsaustausch (Gefährdungshinweise, Tat-Begehungsmuster, Risikobewertung), das in einem 2002 geschlossenen Zusatzabkommen[3] auf die Übermittlung personenbezogener Daten (Namen, Adressen und Kriminalakten von Verdächtigen) ausgeweitet wurde.

Von Interesse waren für die US-Behörden auch Informationen über Flugpassagiere (PNR-Daten) und über Finanztransaktionen. Dem Verlangen nach einem umfassenden Datenzugriff wurde seitens Europas zunächst überwiegend ohne rechtliche Grundlage stattgegeben. So setzten die USA den Zugriff auf die PNR-Daten mit der Drohung durch, ansonsten den widerspenstigen Airlines die Landegenehmigungen in den USA zu entziehen. Der Zugriff auf die Daten der weltweiten Finanztransaktionen, die durch das belgische Unternehmen SWIFT abgewickelt wurde, erfolgte zunächst heimlich. Bei Nichtbefolgung der entsprechenden Anordnungen des US-Finanzministeriums wurden dem Unternehmen – wie zuvor den Fluggesellschaften – empfindliche Sanktionen angedroht. SWIFT kam diesen Forderungen nach, konnte aber gewisse Einschränkungen und Sicherheitsmaßnahmen aushandeln. Erst auf Grund von Presseberichten Mitte 2006 erfuhr die Öffentlichkeit von dieser Angelegenheit. Im Zuge der folgenden Diskussion mussten die Europäische Zentralbank (EZB), einige nationale Zentralbanken (darunter auch die Deutsche Bundesbank) und die im SWIFT-Vorstand repräsentierten Bankenkonsortien einräumen, dass sie von der Übermittlung der Bankdaten an US-Behörden wussten. Zu ihrer Verteidigung führten sie an, sie

hätten an der Rechtmäßigkeit der Zugriffe nicht gezweifelt.

Die robuste Praxis der US-Sicherheitsbehörden und die Willfährigkeit der europäischen Seite trafen in der Öffentlichkeit und auch im Europäischen Parlament auf zunehmende Kritik, da offensichtlich war, dass die Datenübermittlungen vielfach dem Recht der Europäischen Union widersprachen. Insbesondere im Rat und in der Kommission setzte sich die Position durch, die zweifelhaften Datenzugriffe zwar – auch vor dem Hintergrund der schweren terroristischen Anschläge in Madrid (2004) und London (2005) – weiterhin zuzulassen, sie aber zugleich durch bilaterale Abkommen zwischen der EU und den USA rechtlich abzusichern und einzuhegen. Zeitgleich verfolgten die EU-Gremien das Ziel, den Austausch von polizeilichen und justiziellen Informationen zwischen den Behörden der Mitgliedstaaten nach dem „Grundsatz der Verfügbarkeit“ zu erleichtern („Schwedische Initiative“).[4]

2. Bilaterale („Prüm-like“) Abkommen der USA mit EU-Mitgliedstaaten

Unabhängig von den Bemühungen zur Absicherung und Intensivierung des Datenaustauschs auf EU-Ebene drängte die US-Regierung auf vertragliche Festlegungen mit den einzelnen EU-Staaten, die den transatlantischen Datenfluss garantierten und ausweiteten. Bilaterale Vereinbarungen mit einzelnen Staaten waren aus US-Sicht auch deshalb vorteilhaft, weil deren individuelle Verhandlungsmacht schwächer eingeschätzt wurde als diejenige der EU-Institutionen. Andererseits boten solche Vereinbarungen den Regierungen der Mitgliedstaaten die Möglichkeit, sich als besonders zuverlässige Bündnispartner der USA im Krieg gegen den Terrorismus zu profilieren. Ein wirksames US-Argument gegenüber den neuen (osteuropäischen) EU-Mitgliedstaaten war zudem die Aussicht, deren Bürger nach Abschluss bilateraler Abkommen in das „Visa Waiver“-Programm einzubeziehen, das eine visafreie Einreise in die Vereinigten Staaten gestattet.[5]

Eine Art Blaupause für die bilateralen Abkommen war das am 27. Mai 2005 von den Regierungen von sieben EU-Mitgliedstaaten im Luxemburger Städtchen Prüm unterzeichnete Abkommen über die gegenseitige grenzüberschreitende polizeiliche Zusammenarbeit („Prümer Vertrag“), das im Jahr 2008 in Unionsrecht überführt wurde.[6] Wesentlicher Regelungsgehalt des Prümer Vertrags ist die grenzüberschreitende Zusammenarbeit bei der Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration. Zu diesen Zwecken wurde der Austausch auch personenbezogener Daten intensiviert, u. a. durch gegenseitigen Zugriff auf daktyloskopische und auf DNA-Indexdateien und durch Übermittlung personenbezogener Daten zur Verhinderung terroristischer Straftaten. Zur Wahrung der Bürgerrechte verpflichten sich die Vertragsparteien zur Einhaltung eines hohen Datenschutzstandards. Dazu gehören ein einheitlicher Mindeststandard beim Datenschutz, die Zweckbindung der übermittelten Daten und die Gewährleistung der Rechte der Betroffenen, u. a. der Rechte auf Auskunft und auf Schadensersatz.

Am 1. Oktober 2008 unterzeichneten Regierungsvertreter der USA und Deutschlands ein bilaterales („Prüm-like“) Abkommen über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität.[7] Beide Staaten räumten sich darin einen gegenseitigen Zugriff auf daktyloskopische Daten und DNA-Profile und auf entsprechende Fundstellendatensätze ein. Zudem wurden die Regelungen des Prümer Vertrages zum Austausch personenbezogener Daten zur Verhinderung von terroristischen Straftaten weitgehend übernommen. Auf eine Übertragung der als Bedingung für diese umfangreichen Zugriffs- und Übermittlungsbefugnisse im Prümer Vertrag geschaffenen Datenschutzregelungen wurde jedoch weitgehend verzichtet.[8] Entsprechende Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder blieben unberücksichtigt.[9] Insbesondere hatten die Datenschutzbeauftragten das Fehlen jeglicher Betroffenenrechte für die Verarbeitung übermittelter Daten in den USA moniert. In den USA würden Datenschutzrechte, wie sie in der Europäischen Union allen Menschen zustehen, ausschließlich Bürgerinnen und Bürgern der Vereinigten Staaten von Amerika und dort wohnenden Ausländerinnen und Ausländern gewährt. Zudem fehle in den USA eine unabhängige Datenschutzkontrolle. Diese Mängel seien deshalb besonders gravierend, weil in den USA polizeiliche Daten über Jahrzehnte gespeichert würden. Sie würden auch nicht durch das Vertrags- und Umsetzungsgesetz zu dem Regierungsabkommen[10] ausgeglichen.

Die Tatsache, dass die USA in den Folgejahren ähnliche Abkommen („Prüm-like agreements“) ohne hinreichende Datenschutzgarantien mit weiteren EU-Staaten abschlossen, führte zu Forderungen nach vertraglichen Regelungen zwischen der EU und den USA, welche die Mängel dieser Abkommen ausgleichen und einen angemessenen Datenschutz für die aus der EU übermittelten Daten garantieren sollten. Zugleich wuchsen die Zweifel daran, ob die zwischen der EU und den USA geschlossenen Abkommen zum Datenaustausch über Finanztransaktionen[11] und zur Übermittlung von Flugpassagierdaten[12] zur Kriminalitäts- und Terrorismusbekämpfung den Anforderungen der EU-Grundrechtecharta genügten, die durch den am 1. Dezember 2009 in Kraft getretenen Vertrag von Lissabon zum verbindlichen Recht in der gesamten EU geworden waren.

3. Das Umbrella-Agreement

Am 3. Dezember 2010 billigten die EU-Justizminister die Aufnahme von Gesprächen mit den USA über ein entsprechendes Rahmenabkommen zum Schutz personenbezogener Daten. Die EU-Kommission hatte den Entwurf eines entsprechenden Verhandlungsmandats am 26. Mai 2010 vorgelegt. Durch das Rahmenabkommen („Umbrella Agreement“) solle der Bürger in seinem Recht gestärkt werden, Auskunft über persönliche Daten zu erhalten, die zum Zwecke der Verhinderung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten einschließlich solcher mit terroristischem Hintergrund verarbeitet wurden, und diese gegebenenfalls berichtigen oder löschen zu lassen.[13]

Die Verhandlungen zogen sich über Jahre hin und vielen Beobachtern drängte sich der Eindruck auf, dass die US-Seite

an einem positiven Verhandlungsergebnis überhaupt nicht interessiert seien.[14] Deshalb war die Meldung am 8. September 2015 über einen erfolgreichen Abschluss der Verhandlungen mit den USA über ein Datenschutz-Rahmenabkommen durchaus überraschend. Vermutlich haben die als Folge der Enthüllungen über die globalen Überwachungsaktivitäten der National Security Agency (NSA) zunehmenden Zweifel an der Vereinbarkeit der bestehenden Abkommen und Verfahren zur Datenübermittlung an US-Behörden mit den EU-Grundrechten[15] die Bereitschaft der US-Seite zu einem Entgegenkommen erhöht.

Das Abkommen werde nach seinem Inkrafttreten „ein hohes Datenschutzniveau für alle personenbezogenen Daten garantieren, die von den Strafverfolgungsbehörden über den Atlantik gesandt werden. Insbesondere wird es garantieren, dass alle EU-Bürger das Recht haben, den Schutz ihrer Daten bei US-Gerichten durchzusetzen“, führte die zuständige EU-Justizkommissarin Věra Jourová aus.[16] Voraussetzung für die Unterzeichnung der Vereinbarung sei jedoch, dass der US-Kongress die erforderlichen Gesetzesänderungen („Judicial Redress Act“ – JRA) beschließe. Inzwischen hat das Repräsentantenhaus den vom republikanischen Kongress-Abgeordneten James Sensenbrenner jr. eingebrachten Gesetzentwurf gebilligt. Eine Verabschiedung durch den Senat steht noch aus.[17]

Obwohl die Kommission den vereinbarten Text zunächst nicht veröffentlichen wollte, ist dieser – auf welchen Wegen auch immer – ins Internet gelangt[18] und ermöglicht so die erforderliche Detailprüfung.

4. Unzureichender Schutz

Die Durchsicht des Vertragstextes führt zu einem zwiespältigen Ergebnis. Positiv ist, dass das Abkommen in der Tat substantielle Zugeständnisse der US-Seite enthält, die von vielen Beobachtern vor Jahresfrist kaum für möglich gehalten wurden. Zu nennen ist in erster Linie, dass EU-Bürger zukünftig vor US-Gerichten überhaupt einklagbare Datenschutz-Rechte erhalten sollen. Gegen eine derartige Regelung hatte sich die US-Regierung während der sich über fünf Jahre hinziehenden Verhandlungen lange gewehrt. Statt eines einklagbaren Rechtsanspruches sollten – so die ursprüngliche US-Position – EU-Bürgern Datenschutzrechte nur durch eine Verwaltungsvereinbarung eingeräumt werden. Dass eine – allein vom Goodwill der US-Administration abhängige – Zusicherung kein angemessenes Datenschutzniveau gewährleisten kann, wurde zu Recht von EU-Seite immer wieder betont. Insofern ist es positiv, dass die entsprechenden Rechtsansprüche in einem formellen, durch den US-Kongress zu beschließenden Gesetz, gesichert werden sollen.

Positiv ist auch, dass sich beide Seiten zu den Grundsätzen der Verhältnismäßigkeit, Erforderlichkeit und Zweckbindung beim Umgang mit personenbezogenen Daten bekennen und dass sie sich verpflichten, die Verwendung und die Dauer der Speicherung entsprechend dieser Grundsätze durch Rechtsvorschriften festzulegen.

Allerdings kann von einer rechtlichen Gleichstellung der EU-Bürgerinnen und -Bürger mit US-Bürgern nicht die Rede sein, wie ein Blick in den noch nicht abschließend vom US-Kongress gebilligten Entwurf des Judicial Redress Act (JRA)[19] zeigt. Dabei hätte sich dies sehr leicht in die bestehenden US-Datenschutzvorschriften einfügen lassen: So hätte es genügt, die Regelungen – etwa des US Privacy Act von 1974[20] –, die sich bisher auf US-Bürger und dort rechtmäßig ansässige Ausländer beschränken, auf EU-Bürger zu erweitern. Entsprechende Forderungen hatten etwa die US-Bürgerrechtsorganisationen aufgestellt.[21] Stattdessen enthalten der Abkommenstext und der JRA komplizierte Regelungen, welche im Ergebnis die Gleichstellung nicht gewährleisten. So müssen EU-Bürger ohne dauerhaften Aufenthaltsstatus in den USA – anders als US-Personen – zunächst versuchen, ihre Datenschutzrechte auf dem Verwaltungsweg durchzusetzen. Erst wenn sie damit endgültig gescheitert sind, dürfen sie ein US-Gericht anrufen. Zudem beschränken sich die in Art. 18 des Abkommens vorgesehenen Klagemöglichkeiten auf die ausdrücklich im Abkommen genannten Rechte auf Auskunft und Korrektur der jeweiligen personenbezogener Daten. EU-Bürger haben – anders als US-Bürger – weiterhin keine darüber hinausgehenden Möglichkeiten, die Rechtmäßigkeit des gesamten Verfahrens der Datenverarbeitung gerichtlich überprüfen zu lassen.

Der JRA garantiert den EU-Bürgern zudem nicht einmal diese Datenschutzrechte, sondern er ermächtigt den US-Generalstaatsanwalt (zugl. Justizminister, PSch) lediglich dazu, im Einvernehmen mit anderen Ministerien den Bürgern eines Staates oder eines Wirtschaftsraums die beschriebenen Rechte einzuräumen. Der Justizminister kann die Entscheidungen jederzeit widerrufen, etwa wenn der jeweilige Staat die Datenweitergabe an US-Behörden verweigert oder diese erschwert.

Ein weiterer schwerwiegender Einwand gegen die Vereinbarung richtet sich dagegen, dass das Abkommen keine generelle Klausel zum Schutz der Menschenrechte enthält. Insofern ist nicht ausgeschlossen, dass die aus Europa stammenden Daten durch US-Behörden oder durch die Behörden von Drittstaaten für die Begehung von Menschenrechtsverletzungen verwendet oder weitergeleitet werden, einschließlich willkürlicher Verhaftungen, Folter oder extralegaler Tötungen.[22]

Eine zusätzliche Beschränkung soll nicht unerwähnt bleiben: Während nach dem europäischen Datenschutzrecht und Art. 8 der EU-Grundrechtecharta sämtliche personenbezogenen Daten unabhängig von der Nationalität der Betroffenen geschützt werden, sollen die begrenzten, durch das Abkommen und den JRA beschriebenen Datenschutzrechte nur für EU-Bürger gelten, deren Daten von europäischen Behörden oder Unternehmen auf Basis von bi- oder multilateralen Vereinbarungen an US-Strafverfolgungsbehörden übermittelt wurden, nicht jedoch für Bürgerinnen und Bürgern aus Nicht-EU-Staaten, deren Daten ebenfalls aus der EU stammen.

Schließlich bleibt der Abkommenstext hinsichtlich der Datenschutzaufsicht hinter dem EU-Recht (insb. Art. 8 Abs. 3 der EU-Grundrechte-Charta) zurück: Es fehlt eine ausdrückliche Verpflichtung beider Vertragsparteien, für eine unabhängige Datenschutzaufsicht zu sorgen. Während sich die Europäische Union in dem Abkommen dazu verpflichtet, dass die

unabhängigen Datenschutzbehörden die Rechtmäßigkeit der Datenverarbeitung überprüfen können, verweist das Abkommen hinsichtlich der USA auf eine Vielzahl, teils nicht unabhängiger Kontrollinstitutionen, welche die Datenschutzkontrolle „kumulativ“ ausüben sollen.

5. Fazit

Angesichts dieser Defizite des Rahmenabkommens und des zu seiner Umsetzung vorgesehenen US-Judicial Redress Act erscheint es sehr zweifelhaft, dass damit hinsichtlich der in die Vereinigten Staaten für Zwecke der Strafverfolgung und der Abwehr des Terrorismus übermittelten personenbezogenen Daten ein Schutzniveau garantiert wird, das den Vorgaben der EU-Grundrechtecharta genügt. Die europäischen Gremien, die der Ratifizierung des Abkommens zustimmen müssen, allen voran das Europäische Parlament und die Parlamente der Mitgliedstaaten, sind aufgerufen, das Abkommen gründlich zu prüfen. Gegebenenfalls müssen sie darauf bestehen, dass nachverhandelt wird.

1 Vgl. Kristin Archick, U.S.-EU Cooperation Against Terrorism, Congressional Research Service, 01.12.2014, S. 6.

2 Agreement between the United States of America and the European Police Office v. 06.12.2001, https://www.europol.europa.eu/sites/default/files/flags/united_states_of_america.pdf, letzter Zugriff am 24.01.2016.

3 https://www.europol.europa.eu/sites/default/files/flags/supplemental_agreement_between_europol_and_the_usa_on_exchange_of_personal_data_and_related_information.pdf, letzter Zugriff am 24.01.2016.

4 Europäische Kommission, Memo v. 12.10.2005, http://europa.eu/rapid/press-release_MEMO-05-367_de.htm, letzter Zugriff am 25.01.2016.

5 Vgl. Rocco Bellanova, The Case of the 2008 German-US Agreement on Data Exchange: An Opportunity to Reshape Power Relations?, in: Gutwirth/Poullet/de Hert (Hrsg.), Data protection in a profiled world, Dordrecht 2009, 214.

6 Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0001:0011:DE:PDF – letzter Zugriff: 25.01.2016; vgl. auch Thilo Weichert: Wo liegt Prüm? – Der polizeiliche Datenaustausch in der EU bekommt eine neue Dimension. In: Datenschutz Nachrichten 1/2006, S. 12; Peter Schaar: Datenaustausch und Datenschutz im Vertrag von Prüm. In: Datenschutz und Datensicherheit 30 (2006), 691.

7 Abkommen zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität v. 01.10.2008, https://www.jurion.de/Gesetze/Krim-BAbk_US?from=0:3827937,2,20090905#fn_1_N30052, letzter Zugriff 21.01.2016. Das Abkommen ist am 19.04.2011 in Kraft getreten, vgl. BGBl. 2012 II S. 499.

8 BfDI, 22. TB, S. 136.

9 Vgl. Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, „Unzureichender Datenschutz beim deutsch-amerikanischen Abkommen über die Zusammenarbeit der Sicherheitsbehörden“, 03./04.04.2008.

10 BGBl. 2009 II S. 1010, 1011; Regierungsentwurf: Bundestags-Drucksache 16/13124 v. 25.05.2009.

11 Abkommen zwischen der EU und den USA über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus („TFTP-Abkommen“) , EU-Abl. L 008 v. 13.01.2010 S. 11.

12 Abkommen über die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security („PNR-Abkommen“), EU-ABl. L 204 v. 04.08.2007, S. 18.

13 Europäische Kommission, Presseerklärung v. 03.12.2010, http://europa.eu/rapid/pressrelease_IP-10-1661_de.htm.

14 Vgl. auch Archick, a.a.O. S. 8.

15 Entschließung des Europäischen Parlaments zu dem Überwachungsprogramm der NSA der Vereinigten Staaten, den Überwachungsbehörden in mehreren Mitgliedstaaten und den entsprechenden Auswirkungen auf die Privatsphäre der EU-Bürger (2013/2682(RSP)) v. 04.07.2013, http://www.europarl.europa.eu/me https://www.europol.europa.eu/sites/default/files/flags/united_states_of_america.pdf etdocs/2009_2014/documents/ta/04/07/2013%20-%200322/p7_ta-prov%282013%290322_de.pdf, letzter Zugriff am 25.01.2016.

16 European Commission – Statement by EU Commissioner Věra Jourová on the finalisation of the EU-US negotiations on the data protection „Umbrella Agreement“, 8.9.2015, http://europa.eu/rapid/press-release_STATEMENT-15-5610_en.htm, letzter Zugriff 23.01.2016.

17 Vgl. H.R.1428 – Judicial Redress Act of 2015, https://www.congress.gov/bill/114thcongress/house-bill/1428, letzter Zugriff am 23.01.2016.

18 Agreement between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, detection, and Procesution of Criminal Offenses, http://statewatch.org/news/2015/sep/eu-us-umbrella-agreement-full-text.pdf, letzter Zugriff am 23.01.2016. 19S. Fn. 17.

20 Privacy Act of 1974, 5 U.S.C. § 552a (2012).

21 Vgl. Statement of EPIC on H.R. 1428, the Judicial Redress Act of 2015 v. 16.09.2015, https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf, letzter Zugriff 14.01.2016.

22 Vgl. Douwe Korff, EU-US Umbrella Data Protection Agreement: Detailed analysis, 14.10.2015, http://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/, letzter Zugriff 24.01.2015.

Thilo Weichert

Die EU-Richtlinie für den Datenschutz bei Polizei und Justiz

1 Einleitung

Als am 15.12.2015 die Trilog-Verhandlungen über die grundlegende Reform des europäischen Datenschutzrechts abgeschlossen waren, berichteten die Medien umfassend über die Europäische Datenschutzgrundverordnung (EU-DSGVO), also das künftig gültige allgemeine Datenschutzrecht in der Europäischen Union (EU). Praktisch keine Beachtung fand der kleine Bruder dieser Regelung, über den sich Parlament, Rat und Kommission der EU zeitgleich einigten: die EU-Richtlinie für den Datenschutz bei Polizei und Justiz – genauer die „Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr“. Das Dokument war und ist im Netz von der EU derart versteckt abgelegt, dass der grüne Europaabgeordnete Jan-Phillipp Albrecht dieses leichter zugänglich veröffentlichen musste:

https://www.janalbrecht.eu/fileadmin/material/Dokumente/DPD_consolidated_LIBE-vote-2015-12-17.pdf

Natürlich hat die EU-Richtlinie für Polizei und Justiz (im Folgenden zitiert als „Richtlinie“) nicht die gleiche Relevanz wie die EU-DSGVO, doch ist sie ein Meilenstein für den europäischen Datenschutz in diesem Sektor. Der Datenschutz in den hochsensiblen und eingriffsintensiven Bereichen Strafverfolgung und Gefahrenabwehr wird sich künftig europaweit hieran orientieren. Die Mitgliedstaaten werden in dieser Richtlinie zur Gesetzgebung über die polizeiliche und strafverfolgende Datenverarbeitung verpflichtet. In Deutschland betrifft dies nicht nur den Bund, sondern insbesondere auch die für das allgemeine Polizeirecht zuständigen Bundesländer. Es gibt also genug Gründe, sich die Richtlinie genau anzusehen.

2 Geschichte

Der Vorschlag der EU-Kommission vom 25.01.2012 für eine grundlegende Reform des europäischen Datenschutzrechts umfasste neben dem Entwurf einer EU-DSGVO auch den einer Richtlinie für Polizei und Justiz, mit welcher der Rahmenbeschluss der EU-Kommission 2008/977/JI (ABl. L 350 v. 30.12.2008, S. 60) ersetzt werden soll (2012/0010 (COD)). Die Datenverarbeitung durch Polizei und Justiz gehörte früher der „dritten Säule“ der EU an, die bei weitem nicht so stark reguliert war wie die übrige staatliche Verwaltung und die Wirtschaft. Der bis heute gültige Rahmenbeschluss beschränkt sich ausschließlich auf den grenzüberschreitenden Datenverkehr und machte keinerlei Aussagen über die interne Organisation der Datenverbreitung bei Polizei und Justiz. Dies lässt sich nicht mehr aufrecht halten. Mit den Verträgen von Lissabon wurde dieser Bereich „vergemeinschaftet“. In diesem Zusammenhang wurde Ende 2009 auch die Europäische Grundrechtecharta (EUGRCh) in Kraft gesetzt, die in den Art. 7, 8 und 47 Privatsphäre, Telekommunikationsgeheimnis, Datenschutz und einen effektiven Rechtsschutz zusichern. Diese Garantien gelten auch für die Bereiche der Strafverfolgung und der Gefahrenabwehr.

Im sog. Stockholmer Programm (ABl. C 115 v. 04.05.2010, S. 1) hatte der Rat der EU die Kommission ersucht, die bestehenden Rechtsinstrumente zum Datenschutz zu bewerten und im Bedarfsfall Initiativen vorzulegen. Die EU-Kommission erstellte einen Aktionsplan zur Umsetzung des Stockholmer Programms (Com(2010) 171 endg.), in dem zwecks „konsequenter Anwendung des Grundrechts auf Datenschutz“ eine Stärkung der „Position der EU bezüglich des Schutzes personenbezogener Daten bei allen EU-Maßnahmen, einschließlich jener in den Bereichen Strafverfolgung und Kriminalprävention sowie in unseren internationalen Beziehungen“ vorgesehen ist.

In Art. 16 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) ist der Grundsatz verankert, dass jede Person das Recht auf Schutz ihrer personenbezogenen Daten hat. Art. 16 Abs. 2 AEUV schafft eine besondere Rechtsgrundlage für den Erlass von Datenschutzvorschriften, die auch für die polizeiliche und justizielle Zusammenarbeit in Strafsachen gilt. Vom 04.11.2010 bis 15.01.2011 erfolgte eine Konsultation zum Gesamtkonzept der Kommission für den Datenschutz in der EU. Mit Entschließung vom 06.07.2011 nahm das EU-Parlament einen Bericht an, der das Kommissionskonzept für die Reform des Datenschutzes unterstützt.

Ähnlich wie bei der EU-DSGVO stand auch bei der geplanten Regulierung im Bereich Polizei/Justiz das in Art. 5 Abs. 3 EU-Vertrag (EUV) niedergelegte Subsidiaritätsprinzip zur Diskussion, wonach die EU nur tätig werden darf, sofern und soweit die angestrebten Ziele von den Mitgliedstaaten allein nicht ausreichend verwirklicht werden können und wegen ihres Umfangs und ihrer Wirkung auf Unionsebene besser zu verwirklichen sind. Der Deutsche Bundesrat erhob Subsidiaritätsrügen gegen die EU-DSGVO und die Richtlinie. Beides wurde von der EU zurückgewiesen.

Da der Bedarf der Strafverfolgungsbehörden an einem schnellen Datenaustausch zur Verhütung und Bekämpfung von Kriminalität ein unionsweites einheitliches Datenschutzniveau erfordert, sei eine Regulierung nötig. Eine Richtlinie wurde als einzig verhältnismäßig angesehen, um den Mitgliedstaaten bei der Umsetzung der Grundsätze und der Vorschriften noch einen Spielraum zu belassen. Neben den schon erwähnten Grundrechten aus Art. 7, 8 und 47 EUGRCh ist das Diskriminierungsverbot im Hinblick auf Rasse, ethnische Herkunft, genetische Merkmale, Religion, Weltanschauung, politische oder sonstige Anschauung, Behinderung und sexuelle Ausrichtung (Art. 21 EUGRCh) von Relevanz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder gab am 11.06.2012 eine Stellungnahme zum Kommissionsentwurf ab. Die Artikel-29-Arbeitsgruppe erstellte auch eine Stellungnahme mit Datum vom 26.02.2013 mit den vier Schwerpunkten: Verarbeitung von Daten nichtverdächtiger Personen, Betroffenenrechte, Datenschutzfolgenabschätzung und Befugnisse der Datenschutzaufsicht.

Der Vorschlag der EU-Kommission wurde intensiv vom EU-Parlament behandelt und am 12.03.2014 mit Änderungsvorschlägen mit großer Mehrheit angenommen. Berichterstatter war der griechische Abgeordnete Dimitros Droutsas. Die daraufhin erfolgende Behandlung im EU-Rat wurde am 09.10.2015 abgeschlossen.

3 Inhalt der Richtlinie

Zum Zeitpunkt des Verfassens dieses Artikels lag noch keine deutschsprachige Version der Richtlinie vor und auch noch kein Beschlusstext mit der endgültigen Durchnummerierung der Artikel und der erläuternden Erwägungsgründe (EG). Die Gliederung der Richtlinie kann der Aufstellung am Ende dieses Beitrags entnommen werden. Dabei wird die Zählweise der Artikel sowohl im Rahmen der Entwurfsbehandlung wie auch in der voraussichtlichen Beschlussfassung dargestellt. Bei der folgenden Darstellung wird die erwartete künftige Artikel-Zählung zu Grunde gelegt.

Die Richtlinie gibt nur einen Regelungsrahmen vor, bei dem den EU-Mitgliedstaaten weitgehende Spielräume gelassen werden. Es wird definitiv klargestellt, dass die nationalen Regelungen ein höheres Schutzniveau als von der Richtlinie vorgegeben gewähren dürfen (Art. 1 Abs. 2). Die Vagheit vieler Regelungen führt dazu, dass es den Mitgliedstaaten oft erlaubt wird, nationale Ausnahmen von Schutzvorschriften vorzusehen.

3.1 Anwendungsbereich

In Art. 1 wird der Gegenstand der Regelung dargestellt: Es geht um den ungehinderten Austausch personenbezogener Daten zwischen Behörden der Polizei und der Justiz innerhalb der EU und den Grundrechtsschutz der davon betroffenen Personen, insbesondere den Datenschutz. Erfasst werden nur Verarbeitungen, die folgende Zwecke verfolgen: „Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder die Durchführung von Kriminalstrafen, einschließlich der Schutz vor und die Verhütung von Gefahren für die öffentliche Sicherheit“ (Art. 1 Abs. 1). Werden von privaten oder öffentlichen Stellen andere Zwecke verfolgt, so ist die EU-DSGVO anzuwenden (Art. 9 Abs. 2). Was unter öffentlicher Sicherheit verstanden wird, ist nicht eindeutig definiert. Erfasst sein sollen auch Zwangsmaßnahmen der Polizei bei Demonstrationen, Sportereignissen und Unruhen (EG 11a/12). Keine Anwendung findet die Richtlinie für EU-Institutionen sowie für Vorgänge, die nicht unter EU-Recht fallen (Art. 2 Abs. 3). Nicht erfasst sein sollen zudem Maßnahmen für die nationale Sicherheit (EG 11b/14). Dies bedeutet, dass neben dem Verteidigungsbereich in Deutschland wohl auch die Inlands- und Auslandsgeheimdienste (VerfSch, MAD, BND) ausgenommen sein sollen. Dass und weshalb Eurojust und Europol ausgenommen werden, ist nicht erkennbar.

Schon aus der gemeinsamen Behandlung von EU-DSGVO und der Richtlinie zeigt sich, dass beide Rechtsmaterien eng aufeinander abgestimmt sind und sich gegenseitig ergänzen sollen. Dies führt zu Parallelen bei den Begriffsbestimmungen (Art. 3), bei der Verantwortlichkeit (Art. 19 ff.), bei den internen Datenschutzbeauftragten (Art. 32-34) oder bei den Aufsichtsbehörden (Art. 41 ff.). Die Richtlinie ist nicht nur bei Polizei und Staatsanwaltschaften anwendbar, sondern auch auf Gerichte, außer wenn diese in ihrer unabhängigen gerichtlichen Funktion tätig sind. National darf geregelt werden, dass selbst unabhängige Strafverfolgungsbehörden ausgenommen werden können (EG 55/80). Dies gilt aber nicht für Deutschland, da hier, entgegen mancher staatsanwaltlichen Behauptung, keine solche quasi-richterliche Unabhängigkeit besteht. Erfasst wird nicht nur die automatisierte, sondern auch die Datenverarbeitung in analogen Dateien (Art. 2 Abs. 2).

3.2 Zulässigkeit der Datenverarbeitung

In Art. 4 Abs. 1 werden die Grundprinzipien der Datenverarbeitung bzw. des Datenschutzes dargestellt, u. a. die Zweckbindung, die Verhältnismäßigkeit („angemessen“, „nicht exzessiv“) und die Erforderlichkeit. Die Zweckänderung wird unter einen nicht erkennbar eingeschränkten nationalen Gesetzesvorbehalt gestellt (Art. 4 Abs. 2).

Die Richtlinie enthält keine eigenständigen Erlaubnisnormen, sondern macht nur Vorgaben hierfür, die in den Mitgliedstaaten erlassen werden. Da in Deutschland insofern ein umfassendes Regelungsregime besteht, das in den wesentlichen Aspekten inhaltlich der Richtlinie entspricht, kann der bestehende Rahmen beibehalten werden. Die Richtlinie differenziert auch nicht danach, ob und wie Daten verdeckt erhoben werden. Hinsichtlich sensibler Daten werden eine strenge Erforderlichkeitsprüfung und zusätzliche Sicherungen gefordert (Art. 8, 9 Abs. 2 u. 3). Detailliertere Anforderungen an die nationalen Normen oder (Beweis-) Verwertungsverbote sind nicht vorgesehen. Ebenso fehlen, wie vorgeschlagen wurde, Aussagen über auf Einwilligung basierende Datenverarbeitungen.

Angesichts der Weite der vorgegebenen materiellen Regelungen wird es jetzt darauf ankommen, welche Grenzen der Europäische Gerichtshof (EuGH) angesichts Art 8 EUGRCh, der als Maßstab für die Auslegung der gesamten Richtlinie herangezogen werden kann, setzt (s. u. 5).

Anders als zunächst im Kommissionsvorschlag ist in Art. 5 vorgesehen, dass im nationalen Recht Lösch- und Prüffristen und entsprechende Verfahren geregelt werden müssen. Art. 6 sieht vor, dass hinsichtlich der Rollen der Betroffenen bei der Verarbeitung differenziert wird, und zwar ob diese erfasst sind als Verdächtige, Verurteilte, Opfer, Zeugen, Hinweisgeber. Eine weitere Differenzierung ist nach der sachlichen Richtigkeit und Zuverlässigkeit, also dem Grad der Wahrscheinlichkeit, vorgesehen. Erweist sich die Unrichtigkeit oder Unvollständigkeit, so müssen entsprechende Korrekturen und bei Übermittlungen Benachrichtigungen vorgenommen werden (Art. 7).

3.3 Betroffenenrechte

Zwar sind in Art. 13 umfassende Informationspflichten gegenüber den Betroffenen hinsichtlich verarbeitende Stelle, Zweck, Beschwerde- und Auskunftsrecht, evtl. Rechtsgrundlage, Speicherfrist, Empfänger und verdeckte Erhebung vorgesehen, doch können diese Ansprüche durch nationale Vorschriften wieder ausgehebelt werden, wenn dies in irgendeiner Weise die Aufgabenwahrnehmung oder die Rechte Dritter gefährdet. Besonders problematisch ist, dass es möglich sein soll, ganze Kategorien von Daten von der Informationspflicht auszunehmen (Art. 13 Abs. 4, s. u. 4.1). Entsprechend wird das in Art. 14 vorgesehene Auskunftsrecht in Art. 15 eingeschränkt. Im Verweigerungsfall ist darüber zu informieren, dass die Datenschutzaufsicht eingeschaltet werden kann (Art. 15 Abs. 3 S. 3). Die Datenschutzaufsicht kann auch dafür vorgesehen werden, die Betroffenenrechte wahrzunehmen (Art. 17).

3.4 Verantwortlichkeit

In den Art. 18 ff. sind Regelungen zur Verantwortlichkeit, zur gemeinsamen Verantwortlichkeit (Art. 21) und zur Auftragsdatenverarbeitung (Art. 22) enthalten. Diese entsprechen den bestehenden sowie den in der EU-DSGVO geplanten Regelungen. In Art. 20 wird explizit „Data protection by Design and by Default" geregelt. Pseudonymisierung und Datensparsamkeit werden erwähnt. Danach wird es verpflichtend, den Zugriff auf Daten zweckspezifisch und aufgabenbezogen zu begrenzen. Doch diese Vorgabe wird dadurch relativiert, dass als Konkretisierung nur klargestellt wird, dass Daten grds. nicht einer unbegrenzten Personengruppe bereitgestellt werden dürfen (Art. 20 Abs. 2 S. 2).

Alle Datenverarbeitungsprozesse sind gemäß Art. 24 zu dokumentieren bzgl. Verantwortlichkeit, Datenschutzbeauftragtem, Zweck, Empfängerkategorien, Profiling, Drittstaatenübermittlung, Rechtsgrund, Auftragsdatenverarbeitungen, evtl. Löschfristen und technisch-organisatorischen Sicherungsmaßnahmen. Zudem ist in Art. 25 eine Protokollierungspflicht bei folgenden Vorgängen vorgesehen: Erhebung, Veränderung, Abfrage, Weitergabe, Kombination, Löschung; bei Abfragen und Weiterleitungen sind Zweck und Zeitpunkt und, soweit möglich, die handelnde Person aufzuzeichnen. Dokumentationen sind der Datenschutzaufsicht zur Verfügung zu stellen, Protokolle auf Anfrage. Es besteht eine generelle Pflicht zur Kooperation mit der Aufsicht (Art. 26).

Beim Einsatz neuer Technologien und im Hinblick auf besondere Grundrechtsgefahren ist ein „Data Protection Impact Assessment", also eine Datenschutzfolgenabschätzung, vorgesehen (Art. 27). Ergibt sich hierbei ein hohes Risiko, so muss die Datenschutzaufsicht eingebunden werden. Innerhalb von 6 Wochen nach der Einbeziehung kann, soweit das nationale Recht dies vorsieht, die Aufsicht Warn- und Untersagungsfunktionen wahrnehmen (Art. 28 Abs. 5). Eine Pflicht zur Beteiligung besteht zudem bei der Vorbereitung von regulativen und gesetzgeberischen Maßnahmen (Art. 28 Abs. 2).

Anders als in der EU-DSGVO werden in Art. 29 die Datensicherheitsmaßnahmen als Katalog entsprechend der Anlage zu § 9 BDSG aufgeführt. Die modernen Datenschutz-Schutzziele werden nur ansatzweise oder überhaupt nicht erwähnt. In den Art. 30, 31 ist die unverzügliche „Meldung einer Verletzung", also eine Breach Notification gegenüber der Datenschutzaufsicht und in speziellen engen Fällen gegenüber den Betroffenen vorgesehen. Die Art. 32 bis 34 enthalten verpflichtende Regelungen zur Ernennung, zur Stellung und zu den Aufgaben eines (internen) Datenschutzbeauftragten.

3.5 Datenübermittlung ins Drittausland

In den Art. 35-39 sind die materiellen Anforderungen an Datenübermittlungen in Drittländer geregelt. Grundsätzlich müssen folgende Voraussetzungen vorliegen: Erforderlichkeit, Zuständigkeit des Empfängers, Datenfreigabe durch Herkunftsland bei erhaltenen Daten und angemessenes Datenschutzniveau.

Fehlt es an einem zuvor festgestellten angemessenen Datenschutz beim Empfänger, kann dennoch eine Übermittlung erfolgen, wenn dies unter Berücksichtigung aller Umstände vom Ursprungsland zugelassen wird. Eine weitere Ausnahme von Erfordernis eines hinreichenden Datenschutzstandards besteht bei Erforderlichkeit für die Verhinderung einer unmittelbaren ernsthaften Gefahr für die öffentliche Sicherheit, wenn die Zustimmung des Ursprungslands nicht erlangt werden könnte. Dieses muss nachträglich informiert werden (Art. 35 Abs. 2, 3).

Nicht erwähnt wird, aber selbstverständlich sein sollte, dass Übermittlungen innerhalb der EU wie auch in Drittländer den nationalen Übermittlungsregelungen, wie sie auch zwischen Behörden im eigenen Land gelten, entsprechen müssen. Keine weitergehenden Einschränkungen bestehen, wenn die EU-Kommission festgestellt hat, dass im Empfängerland ein angemessenes Datenschutzniveau besteht. Bei der Kommissionsentscheidung sind folgende Aspekte relevant: rechtsstaatliches Verfahren, eine unabhängige Datenschutzkontrollinstanz und internationale Datenschutzverpflichtungen. Die Kommission muss laufend überprüfen, ob die Voraussetzungen weiterhin vorliegen. Ist dies nicht der Fall, ist die Angemessenheitsfeststellung zurückzunehmen bzw. zu ändern und es sind Verhandlungen mit dem Empfängerland aufzunehmen.

Fehlt es an einer allgemeinen Angemessenheitsfeststellung, so kann die Datenübermittlung mit spezifischen Sicherungen im Einzelfall legitimiert werden (Art. 37). Besteht insofern kein rechtlich bindendes Instrument, so muss die Datenschutzaufsicht informiert werden.

Schließlich dürfen Übermittlungen ohne jede Datenschutzsicherung erfolgen, wenn dies erforderlich ist für den Schutz eines lebenswichtigen Interesses des Betroffenen oder einer anderen Person, bei Vorliegen einer nationalen Regelung zum Schutz legitimer Betroffeneninteressen, zur Verhütung einer unmittelbaren ernsthaften Gefahr für die öffentliche Sicherheit entweder des Mitgliedstaats oder eines anderen Landes, in einzelnen Fällen für Zwecke nach Art. 1 Abs. 1 (Generalklausel) oder im Einzelfall zur Ausübung und Durchsetzung rechtlicher Interessen nach Art. 1 Abs. 1 (Art. 38 Abs. 1). Generell soll gelten, dass eine Übermittlung unzulässig ist, wenn die Behörde feststellt, dass die schutzwürdigen Betroffeneninteressen gegenüber dem öffentlichen Interesse an der Datenübermittlung überwiegen (Art. 38 Abs. 2). Beachtet werden soll, dass das Daten nicht zur Begründung, Verwendung oder Umsetzung einer Todesstrafe oder einer anderen Form grausamer oder unmenschlicher Behandlung genutzt wird (EG 49/71). Die Übermittlung muss mit Zeitangabe, Empfänger und rechtfertigendem Grund dokumentiert werden.

Art. 39 sieht eine weitere Ausnahme im Einzelfall bei Übermittlungen an beliebige Dritte vor, wenn dies unbedingt notwendig ist für die Aufgabenerfüllung der übermittelnden Stelle und diese feststellt, dass Grundrechte gegenüber den öffentlichen Interessen an der Übermittlung nicht überwiegen, eine Übermittlung an die zuständige Stelle im Empfängerland keinen Erfolg verspricht, diese, soweit sinnvoll, informiert wird und dem Empfänger der spezifische Übermittlungszweck mitgeteilt wird. Dies kann in einem internationalen Abkommen vereinbart sein. Die Aufsichtsbehörde der übermittelnden Behörde muss informiert werden (Art. 39).

3.7 Datenschutzaufsicht

Die Art. 41 bis 49 regeln die unabhängige Datenschutzkontrolle. Diese ist an die Regelungen in der EU-DSGVO angelehnt. Sie muss unabhängig sein und mit personellen, technischen und finanziellen Ressourcen ausgestattet sein, um ihre Aufgaben und Befugnisse effektiv umsetzen zu können (Art. 42). Die in der EU-DSGVO vorgesehenen Behörden können auch als Aufsicht im Polizei- und Justizbereich eingesetzt werden.

Die Aufgaben der Datenschutzaufsicht liegen in der Datenschutzkontrolle gemäß Art. 46 der Richtlinie, der Öffentlichkeitsarbeit, der Beratung von Parlament und öffentlichen Stellen, der Fortbildung verantwortlicher Stellen, der Bearbeitung von Betroffenenanfragen und -beschwerden, der Rechtmäßigkeitskontrolle bei der Auskunftserteilung, der (europaweiten und internationalen) Zusammenarbeit mit anderen Aufsichtsbehörden (Art. 50), der Durchführung von Untersuchungen, der Beobachtung relevanter Entwicklungen, der Beratung bei der Datenschutzfolgenabschätzung und der Mitarbeit im Europäischen Datenschutzausschuss (Art. 51).

Die Datenschutzaufsicht hat umfassende Ermittlungsbefugnisse sowie „wirksame Einwirkungsbefugnisse“. Dazu zählen Beanstandungen, Anordnungen an die verantwortliche Stelle im Hinblick auf unzulässige Formen der Datenverarbeitung bis hin zu befristeten oder vollständigen Untersagungen bestimmter Verfahren (Abs. 47 Abs. 1, 2). Außerdem ist im nationalen Recht vorzusehen, dass die Aufsichtsbehörde die Befugnis erhält, Datenschutzverstöße einem justiziellen Verfahren zuzuführen (Art. 47 Abs. 5). Über wirksame Mechanismen muss gewährleistet werden, dass die zuständigen Aufsichtsbehörden vertraulich über Datenschutzverstöße unterrichtet werden können (Art. 48). Mit der Kooperationsbefugnis gegenüber anderen Aufsichtsbehörden korrespondiert eine grds. unentgeltliche Kooperationspflicht (Art. 50 Abs. 4-8). Dem Europäischen Datenschutzausschuss kommen, anders als nach der EU-DSGVO, keine Entscheidungsbefugnisse zu. Die Aufgaben bestehen vielmehr in der Beratung, der Herausgabe von Richtlinien, der Prüfung, der Abgabe von Stellungnahmen, der Förderung von Kooperation, Schulung und Forschung.

3.8 Rechtsschutz und Umsetzung

Gemäß Art. 52 hat jeder Betroffene das Recht, sich mit einer Beschwerde wegen eines möglichen Datenschutzverstoßes an eine Aufsichtsbehörde zu wenden. Ist diese nicht zuständig, so leitet diese die Beschwerde an die zuständige Stelle weiter. Die Aufsichtsbehörde informiert den Betroffenen über den Fortschritt und das Ergebnis der Beschwerde einschließlich der Möglichkeiten für gerichtlichen Rechtsschutz. Gegen Entscheidungen der Aufsichtsbehörde sowie wegen deren Untätigkeit kann gerichtlicher Rechtsschutz erlangt werden (Art. 53). Ein gerichtlicher Rechtsbehelf ist auch gegen die für die Verarbeitung verantwortliche Stelle oder den Auftragsdatenverarbeiter gegeben (Art. 54). Im nationalen Recht ist auch vorzusehen, dass Einrichtungen, Organisationen oder Verbände das Recht haben, im Namen des oder der Betroffenen die Beschwerde- und Klagerechte nach den Art. 52, 53 und 54 wahrzunehmen.

Im nationalen Recht sind zudem Haftungs- und Sanktionsregelungen vorzusehen (Art. 56, 57).

Zur Umsetzung der Richtlinie gibt es ein Ausschussverfahren im Sinne der Verordnung (EU) Nr. 182/2011 (Art. 58). Der Rahmenbeschluss 2008/977/JHA wird aufgehoben (Art. 59). Internationale Abkommen, die vor Inkrafttreten der Richtlinie geschlossen wurden und die mit Unionsrecht in Einklang stehen, bleiben in Kraft, bis diese verändert, ersetzt oder aufgehoben werden (Art. 61). In Art. 62 ist ein umfangreiches Evaluationsverfahren vorgesehen. Die ersten Berichte müssen innerhalb von 4 Jahren nach Inkrafttreten vorgelegt werden. Innerhalb von 3 Jahren sind weitere Regelungen daraufhin zu überprüfen, ob sie angesichts der vorliegenden Richtlinie angepasst werden müssen. Gemäß Art. 63 Abs. 4 teilen die Mitgliedstaaten der EU-Kommission mit, welche Vorschriften sie zur Umsetzung der vorliegenden Richtlinie erlassen haben.

4. Bewertung

So zufrieden man als Datenschützer mit dem Trilog-Ergebnis zur EU-DSGVO sein kann, so wenig ist dies bei der Datenschutzrichtlinie für Polizei und Justiz gerechtfertigt. Zwar ist diese gegenüber dem bisher geltenden Rahmenbeschluss ein Fortschritt. Doch genügen die materiellen Regelungen in

vieler Hinsicht nicht den hohen Anforderungen, die Eingriffe in das Grundrecht auf Datenschutz sowie in andere Grundrechte durch die Polizei und die Justiz stellen. Der Umstand, dass bei der europäischen Datenschutzreform die EU-DSGVO im Vordergrund stand, hat offenbar dazu geführt, dass bei der Richtlinie administrative Verarbeitungsinteressen keiner öffentlichen Kritik ausgesetzt waren und sich deshalb durchsetzen konnten.

Gemäß den Anforderungen des EuGH sind für informationelle Eingriffe „klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme“ nötig, die sich „auf das absolut Notwendige“ beschränkt (EuGH, U. v. 06.10.2015, Rn. 91, 92). Diesen Anforderungen genügt die Richtlinie selbst nicht. Dem muss aber das die Richtlinie umsetzende nationale Recht genügen.

4.1 Mangelhafte Betroffenentransparenz

Besonders defizitär sind die Ausnahmemöglichkeiten bei der Benachrichtigung über verdeckte Maßnahmen bzw. bei der Auskunftserteilung. Diese sehen pauschale Informationsverweigerungen vor, ohne dass eine Abwägung im Einzelfall erforderlich wäre, so in den Art. 13 Abs. 4, 15 Abs. 2. Ohne Kenntnis einer Datenverarbeitung ist es einem Betroffenen unmöglich, sein Grundrecht auf Datenschutz in der Praxis auszuüben. Gerade im Bereich von Strafverfolgung und Gefahrenabwehr haben Behörden umfassende Rechte zur heimlichen Datenerhebung. Umso wichtiger sind Benachrichtigungen und Auskunftsansprüche, um die Rechtsmäßigkeit der informationellen Eingriffe überprüfen (lassen) zu können. Die Ausnahmeregelung in Art. 13 Abs. 3 lit. b, 15 Abs. 1 lit. b „zur Gewährleistung, dass Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten nicht beeinträchtigt“ wird, eröffnet viele Möglichkeiten für willkürliche Informationsverweigerungen. Entsprechendes gilt für die Verweigerung „zum Schutz der öffentlichen Sicherheit“ (Art 13 Abs. 3 lit. c, 15 Abs. 1 lit. c). Die genannten Regelungen genügen nicht den Bestimmtheitsanforderungen, die sich aus Art. 8 Abs. 2 S. 1 und 2 EUGRCh ergeben, wo es heißt: „Jeder Mensch hat das Recht, Auskunft über die ihn betreffenden erhobenen Daten zu erhalten ...“. Die Regelungen stellen nicht sicher, dass, wie im Grundrechtsbereich nötig, eine Abwägung im Einzelfall erfolgt.

Mit den Regelungen wird zudem die in Art. 47 EUGRCh zugesicherte Möglichkeit der Erlangung effektiven Rechtsschutzes beeinträchtigt, dessen Bedeutung der EuGH in der Safe-Harbor-Entscheidung vom 06.10.2015 hervorgehoben hat (C-362/14, Rn. 64, 95).

4.2 Auslandsübermittlung

Es ist äußerst fraglich, ob die Übermittlungsregelungen in Drittländer in den Art.35 ff. grundrechtskonform sind. Zwar enthält Art. 35 Abs. 3 eine salvatorische Abwägungsklausel: „Alle Regelungen dieses Kapitels sind so anzuwenden, dass sichergestellt wird, dass das durch diese Richtlinie garantierte Schutzniveau für den Einzelnen nicht untergraben wird.“ Die dann folgenden Normen greifen aber diesen Grundgedanken nur ungenügend wieder auf. Insbesondere bei den „Ausnahmen in spezifischen Situationen“ gemäß Art. 38 wird nicht in allen Fällen eine Abwägung gefordert (so explizit Art. 38 Abs. 2 mit Bezug auf Abs. 1 lit. a-c).

Die materiellen Voraussetzungen für Datenübermittlungen ohne adäquaten Datenschutz bei den Empfängern sind teilweise äußerst niedrig und allgemein formuliert. Dies ist etwa der Fall bei der „strengen Erforderlichkeit“ für die Aufgabenerfüllung der übermittelnden Stelle in Art. 39 Abs. 1 lit. a. (kritisch hierzu z. B. EuGH, U. v. 06.10.2015, Rn. 86 f.).

Eine adäquate Interessenabwägung wird zudem dadurch in Frage gestellt, dass der Abwägungsvorgang ohne prozedurale Absicherungen regelmäßig durch die verantwortliche übermittelnde Stelle erfolgt, die mit der Übermittlung zumeist ein Eigeninteresse verfolgt. Nur in bestimmten Ausnahmefällen wird eine Informationspflicht gegenüber der Datenschutzaufsicht geregelt (Art. 37 Abs. 2), wobei eine Prüfung im Einzelfall nachschauend nur auf Initiative der Datenschutzaufsicht vorgesehen ist (Art. 37 Abs. 3, 38 Abs. 3). Eine wirksame präventive Sicherungswirkung kann ein solcher Mechanismus nicht entwickeln.

5 Ausblick

Das deutsche Sicherheitsrecht dürfte weitgehend mit den materiell-rechtlichen Anforderungen der Richtlinie übereinstimmen.

Die Regelungen der Richtlinie zum technisch-organisatorischen Datenschutz genügen nicht den aktuellen Anforderungen. Angesichts der weitergehenden Regelungen in der EU-DSGVO sowie in einigen Landesgesetzen sollten sich die deutschen Gesetzgeber in Bund und Ländern weniger an der Richtlinie als an diesen Vorbildern orientieren.

Hinsichtlich der prozeduralen Regelungen zum Datenschutzbeauftragten, zur Datenschutzaufsicht und zum Rechtsschutz besteht auch in Deutschland großer Anpassungsbedarf. Bei diesem Anlass besteht die Möglichkeit, nicht nur die von der Richtlinie geforderten Minimalstandards einzuführen, sondern darüber hinausgehend Defizite der Richtlinie auf der nationalen Ebene zu beheben.

Die Regelungsmaterien des deutschen Polizeirechts werden nicht vollständig von der Richtlinie erfasst, sondern befassen sich auch mit Rechtsfragen, die unter die EU-DSGVO fallen. Dies ist z. B. bei der Fahndung nach Vermissten ohne Bezug auf das Vorliegen einer Straftat der Fall. Um insofern keine Unstimmigkeiten zu bewirken, sollte sich die Umsetzung im Polizeirecht im Zweifel an den jeweils grundrechtsfreundlicheren Regelungen der beiden europarechtlichen Instrumente orientieren.

Die Umsetzung der Richtlinie dürfte wegen der bestehenden europäischen Grundrechtsbindung weitgehend für den EuGH justiziabel sein. In der Safe-Harbor-Entscheidung vom 06.10.2015 hat der EuGH hohe materielle und prozedurale Anforderungen an Auslandsübermittlungen gestellt, insbesondere wenn diese ins Ausland ohne angemessenes Datenschutzniveau erfolgen (C-362/14, Rn. 39, 73-78). Dies muss bei der Umsetzung berücksichtigt werden, wollen die Gesetzgeber auf nationaler Ebene nicht, wie schon oft in der Vergangenheit geschehen, gerichtlich korrigiert werden. Es ist davon auszugehen, dass es in den Mitgliedstaaten bei der grundrechtskonformen Umsetzung der Richtlinie massive Defizite geben wird. Dann liegen alle Hoffnungen beim EuGH, der dies korrigieren kann und muss.

Anhang zum vorstehenden Beitrag:

Inhalt/Gliederung

Europäische Datenschutzrichtlinie für Polizei und Justiz

Erläuterungen:

1. Ziffer = Artikel in den Entwurfsfassungen

2. Ziffer in Klammern = voraussichtliche **Zählung der Artikel** in der Endfassung und **im vorstehenden Beitrag**

Text = Überschrift des Artikels/Kapitels/Abschnitts

3. Ziffer in Klammer = erläuternde Erwägungsgründe (EG) gemäß Entwurfsfassungen

4. Ziffer in Klammer hinter Schrägstrich = voraussichtliche Zählung der Erwägung (EG) in Endfassung

Kapitel 1 Allgemeine Bestimmungen

1 Gegenstand und Ziele (1-5)

2 Anwendungsbereich (6-15b/-20)

3 Begriffsbestimmungen (16-17a, incl. Interpol/21-25)

Kapitel 2 Grundsätze

4 Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten (18-21/25-30)

4b (5) Aufbewahrungsfristen

5 (6) Unterscheidung verschiedener Kategorien von betroffenen Personen (23/31)

6 (7) Unterscheidung von personenbezogenen Daten nach Richtigkeit und Zuverlässigkeit (24/32)

7 (8) Rechtmäßigkeit der Verarbeitung (24a-25a/33-36)

7a (9) Spezifische Verarbeitungsbedingungen (25a/36)

8 (10) Verarbeitung besonderer Kategorien von personenbezogenen Daten (26/37)

9 (11) Auf Profiling und automatischer Datenverarbeitung basierende Maßnahmen (27/38)

Kapitel 3 Rechte der betroffenen Person

10 (12) Modalitäten für die Ausübung der Rechte der betroffenen Person (28-29a/39-41)

10a (13) Information der betroffenen Person (30/42)

12 (14) Auskunftsrecht der betroffenen Person (32/43)

13 (15) Einschränkung des Auskunftsrechts (33-34a/44-46)

15 (16) Recht auf Berichtigung, Löschung und Sperrung (36/47)

15a (17) Ausübung der Betroffenenrechte und Überprüfung durch die Aufsichtsbehörde (36a/48)

17 (18) Rechte der betroffenen Person in strafrechtlichen Ermittlungen und in Strafverfahren (36aa, 82/49, 106)

Kapitel 4 Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter

Abschnitt 1 Allgemeine Verpflichtungen

18 (19) Pflichten des für die Verarbeitung Verantwortlichen (37-37b/50-52)

19 (20) Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen (38/53)

20 (21) Gemeinsam für die Verarbeitung Vantwortliche (39/54)

21 (22) Auftragsverarbeiter (39a/55)

22 (23) Verarbeitung unter der Aufsicht des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters

23 (24) Dokumentation der Verarbeitung (40/56)

24 (25) Aufzeichnung von Vorgängen (40a/57)

25 (26) Zusammenarbeit mit der Aufsichtsbehörde

25a (27) Datenschutzfolgenabschätzung (40b/58)

26 (28) Vorherige Zurateziehung der Aufsichtsbehörde (41/59)

Abschnitt 2 Datensicherheit

27 (29) Sicherheit der Verarbeitung (41a/60)

28 (30) Meldung einer Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde (42/61)

29 (31) Benachrichtigung der betroffenen Person von einer Verletzung des Schutzes personenbezogener Daten (43/62)

Abschnitt 3 Datenschutzbeauftragter (44/63)

30 (32) Benennung des Datenschutzbeauftragten

31 (33) Stellung des Datenschutzbeauftragten

32 (34) Aufgaben des Datenschutzbeauftragten

Kapitel 5 Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen

33 (35) Allgemeine Grundsätze für die Übermittlung personenbezogener Daten (45/64)

34 (36) Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses (45a-48/65-70)

35 (37) Datenübermittlung auf der Grundlage geeigneter Garantien (49/71)

36 (38) Ausnahmen für spezifische Situationen (49aa, 49b/72, 73)

36aa (39) Übermittlung an Empfänger in Drittstaaten

38 (40) Internationale Zusammenarbeit zum Schutz personenbezogener Daten (50/74)

Kapitel 6 Unabhängige Aufsichtsbehörden

Abschnitt 1 Unabhängige Rechtsstellung

39 (41) Aufsichtsbehörde (51-53/75-77)

40 (42) Unabhängigkeit (53a/78)

41 (43) Allgemeine Bedingungen für die Mitglieder der Aufsichtsbehörde (54/79)

42 (44) Vorschriften für die Errichtung der Aufsichtsbehörde

44 (45) Zuständigkeit (55/80)

45 (46) Aufgaben (56-57/81-82)

46 (47) Befugnisse

46a (48) Berichte über eine Verletzung des Schutzes personenbezogener Daten

47 (49) Tätigkeitsbericht

Kapitel 7 Zusammenarbeit

48 (50) Gegenseitige Unterstützung (58/83)

49 (51) Aufgaben des Europäischen Datenschutzausschusses (59/84)

Kapitel 8 Rechtsschutz, Haftung und Sanktionen

50 (52) Recht auf Beschwerde bei einer Aufsichtsbehörde (60/85)

51 (53) Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde (61/86)

52 (54) Recht auf gerichtlichen Rechtsbehelf gegen für die Verarbeitung Verantwortliche oder Auftragsverarbeiter

53 (55) Vertretung von betroffenen Personen (62/87)

54 (56) Recht auf Schadenersatz (64/88)

55 (57) Sanktionen (65/89)

Kapitel 9 Umsetzungsmaßnahmen

57 (58) Ausschussverfahren (67, 68/90, 91); Subsidiarität (70/93)

Kapitel 10 Schlussbestimmungen

58 (59) Aufhebung (71/94)

59 (60) Verhältnis zu bestehenden Rechtsakten der Union im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (72/95)

60 (61) Verhältnis zu bestehenden internationalen Übereinkommen im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (73/96)

61 (62) Bewertung (73a/97 spezifische Mitglieds- und Schengenstaaten 75-79/99-103, Notifikation 81/105)

Jörg Pohle

PERSONAL DATA NOT FOUND:
Personenbezogene Entscheidungen als überfällige Neuausrichtung im Datenschutz



Bei privacy, Privatheit, Privatsphäre, surveillance und Datenschutz handelt es sich unzweifelhaft um essentially contested concepts.[1] Alles an ihnen scheint umstritten, jeder Aspekt umkämpft: Das beginnt schon beim verwendeten Bezeichner, wie die vorstehende Aufzählung zeigt, und geht weiter über den Phänomenbereich und das Schutzgut, den Grund oder die Gründe für dessen Gefährdung sowie das Schutzregime. Eines jedoch scheint für alle Beteiligten sicher zu sein: Das Problem dreht sich irgendwie um personenbezogene Informationen.[2]

Vor dem Hintergrund der Entwicklung, die in den letzten Jahren sowohl die Geschäftsmodelle wie die Technik erfahren haben – von Big Data über Recommender Systems und Predictive Policing bis hin zum Internet of Things –, stellt sich die Frage, ob diese angenommene Selbstverständlichkeit, über personenbezogene Informationen – personenbezogene Daten in der Sprache des Datenschutzrechts[3] – sprechen zu müssen, noch haltbar ist.

Die Antwort darauf lautet – und der Beitrag wird dies zu belegen suchen – nein. Nicht personenbezogene Informationen, sondern personenbezogene Entscheidungen durch Organisationen in strukturell vermachteten Informationsbeziehungen sind zum Anknüpfungspunkt von Datenschutztheorie und Datenschutzrecht zu machen.

Ein Beispiel in vier Fällen

Zur Beantwortung der Frage, ob personenbezogene Informationen ein geeigneter Anknüpfungspunkt für eine Theorie zur Erklärung oder das Recht zur Lösung der oben angedeuteten Probleme im Zusammenhang mit moderner Informationsverarbeitung und Entscheidungsfindung sind, soll folgendes Beispiel dienen: Google entscheidet über Alice. Die Entscheidung, von der hier die Rede ist, kann sich etwa darauf beziehen, welche Informationen Alice als Antwort auf ihre Suchanfrage präsentiert werden und welche nicht, in welcher Reihenfolge die Suchergebnisse angeordnet werden oder welche Werbung dazu jeweils gezeigt wird.[4] Google selbst ist, soviel ist sicher, eine Organisation. Die hier betrachteten Informationsverarbeitungen und Entscheidungsfindungen liegen bei Google nicht in der Hand von Mitarbeiterinnen und Mitarbeitern, sondern sind – jedenfalls so weitgehend wie nur irgend möglich – industrialisiert.[5]

Dieses Beispiel soll nun anhand von vier Fällen analysiert werden.

Im ersten Fall verarbeitet Google personenbezogene Informationen über Alice und trifft die Entscheidungen über Alice auf Basis dieser Informationen. Alice' privacy oder Privatheit ist mindestens tangiert, eventuell – das ist je nach Theorie unterschiedlich – ist sie auch verletzt, jedenfalls aber fällt dieser Sachverhalt unzweifelhaft unter das deutsche und europäische Datenschutzrecht.

Im zweiten Fall trifft Google die Entscheidungen über Alice auf der Basis von Informationen über Bob, die Google zu diesem Zweck verarbeitet. Diese Situation kann etwa eintreten, wenn Alice Bobs Computer nutzt, und Google die Informationen daher als Informationen über Bob verarbeitet, oder wenn Google die Informationen aus anderen Gründen der falschen Person, nämlich

Bob, zuweist. In diesem Fall ist sicher Bobs privacy oder Privatheit betroffen und möglicherweise auch verletzt, aber jedenfalls nicht die von Alice. Die Informationsverarbeitung unterfällt immer noch dem Datenschutzrecht, denn es werden personenbezogene Informationen verarbeitet und genutzt, aber nur Bob hat Betroffenenrechte gegenüber Google, etwa nach §§ 33 ff. BDSG, und Google hat datenschutzrechtliche Pflichten nur gegenüber Bob (und natürlich gegenüber Aufsichtsbehörden), nicht aber gegenüber Alice.

Im dritten Fall basieren Googles Entscheidungen über Alice auf rein statistischen, mithin also nicht personenbezogenen Informationen. Dabei ist unerheblich, was die Basis der statistischen Informationen ist – sie können von vornherein nach § 3a Satz 1 BDSG anonym erhoben oder nach § 3a Satz 2 BDSG nachträglich anonymisiert worden sein und sie können auf Alices Aktivitäten basieren oder auf Aktivitäten von vielen Menschen, die dann zu einer generalisierten Person kondensiert wurden –, denn spätestens mit der nicht wieder aufhebbaren Anonymisierung entfällt „mangels Personenbezug die Anwendbarkeit des Gesetzes ohnehin“.[6] Und auch privacy oder Privatheit von Individuen sind nicht oder nicht mehr betroffen.[7]

Im vierten Fall trifft Google die Entscheidungen über Alice auf der Basis von Informationen, die sich Google einfach ausgedacht hat oder die schlicht reine Sachinformationen sind, etwa Informationen über das Wetter. Wieder handelt es sich nicht um einen privacy- oder privatheitsbezogenen oder dem Datenschutzrecht unterfallenden Sachverhalt.

In allen vier Fällen ist klar, dass die Beziehung zwischen Alice und Google von einer strukturellen Machtimbalance zugunsten Googles geprägt ist: Google entscheidet nach selbst gesetzten – und dabei nicht unbedingt in sich konsistenten oder auf Dauer gestellten – Maßstäben darüber, was Alice über sich selbst, die Gesellschaft, ja die Welt – oder womöglich auch nur über das Internet – wissen oder zumindest finden kann. Dennoch handelt es sich nur im ersten Fall – jedenfalls ausweislich aller privacy-, Privatheits- und Privatsphäretheorien – um ein privacy-, Privatheits- und Privatsphäreproblem für Alice und – von einer Ausnahme im Telemediengesetz abgesehen[8] – einen Fall des Datenschutzrechts.[9]

Das alles heißt aber nichts anderes, als dass Entscheidungen über Menschen in vermachteten Beziehungen nur dann problematisiert werden, wenn diese auf der Basis von Informationen über diese Menschen getroffen werden. Warum sollte es aber substantiell einen Unterschied markieren, dass Google – oder irgendeine andere (informations-)mächtige Organisation – Entscheidungen über Menschen auf der Basis von Informationen über andere Menschen – oder Gruppen oder ganze Bevölkerungen oder das Wetter – trifft als auf der Basis von Informationen über die Menschen selbst, über die Google entscheidet? Was ist dieser Unterschied, der als privacy, Privatheit oder Privatsphäre bezeichnet wird, und was macht ihn schützenswert und geschützt durch das Recht? Keine der existierenden Theorien versucht auch nur, darauf eine Antwort zu geben.[10] Und wenn sie es täte, dann müsste sie wohl sicher scheitern.

Woher kommt die Fixierung auf personenbezogene Informationen?

Die erste Frage, die sich in diesem Zusammenhang stellt, ist die nach dem geschichtlichen Hintergrund der Fixierung der gesamten Debatte wie aller gesetzlichen Regelungsregime auf personenbezogene Informationen. Eine umfassende Analyse der wissenschaftlichen Arbeiten, die im Laufe der privacy-, Privatheits- und Datenschutzdebatte die Richtung der Diskussion beeinflussten, ergibt, dass diese Fixierung wohl drei Ursachen hat: Die erste liegt in einem Übersetzungsplagiat aus dem Urheberrecht, die zweite in der Übernahme der informierten Einwilligung aus dem Bereich medizinischer Eingriffe und die dritte in einer Fehlvorstellung darüber, wie rationale Bürokratien im Weberschen Sinne rationale Entscheidungen treffen.

…aus dem Urheberrecht

Obwohl Hans-Heinrich Maass schon vor Jahrzehnten darauf hingewiesen hat,[11] dass sich Samuel D. Warren und Louis D. Brandeis in ihrer bekannten Arbeit „The Right to Privacy“[12] ziemlich frei bei Josef Kohler und seinem Werk „Das Autorrecht“[13] – vor allem für die Konstruktion ihrer Argumentationsstruktur – bedienten, ohne es zu zitieren, sind dieser Zusammenhang und die daraus resultierenden Folgen für das right to privacy bisher nicht wissenschaftlich untersucht.[14]

Kohler argumentiert in seiner Arbeit, dass aus dem von ihm als schon im Römischen Recht durch die actio iniuriarum, die auch Warren und Brandeis als historischen Bezugspunkt verwenden,[15] als geschützt angesehenen „Individualrecht“ Autorinnen und Autoren das Recht erwachse, „daß ein Jeder alleiniger Herr ist, zu bestimmen, welche Aeußerungen und Kundgebungen er in das Publikum tragen will und welche nicht“.[16] Diese Formulierung, die sich auch bei Warren und Brandeis als „determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others“ findet,[17] ist eng gebunden an den betrachteten Phänomenbereich und den zugrunde gelegten Sachverhalt – sowohl bei Kohler wie auch bei Warren und Brandeis. In dem Bereich, den Kohler betrachtet, geht es um die Frage, wer das Recht habe zu entscheiden, ob ein Werk – die „Aeußerungen und Kundgebungen“ – mit dem Akt der Veröffentlichung einer unbeschränkten Öffentlichkeit zugänglich gemacht werden soll. Während der Angreifer hier ein Verlag ist, der das Werk ohne Zustimmung der Autorin oder des Autors publiziert, ist es im Falle Warren und Brandeis’ die Presse, die „the sacred precincts of private and domestic life“[18] ans Licht der Öffentlichkeit zerrt.

In beiden Fällen ist es demnach der Akt dieser Weitergabe – ob an eine oder mehrere andere Personen oder an eine unbeschränkte Öffentlichkeit –, der einen Eingriff darstellt und damit zugleich zum konstitutiven Element des Konzeptes oder der Theorie gemacht wird, nicht jedoch eine oder mehrere Entscheidungen, die – ob auf der Basis der veröffentlichten Informationen oder nicht – über die Betroffenen getroffen werden. Privacy ist damit von Warren und Brandeis, indem sie sich

im Urheberrecht bedienten, an den ihm zugrunde liegenden Vorgang gebunden worden: ein Etwas, das aus dem „Innersten“ der oder des Betroffenen kommt, und für das die Entscheidung über deren Verbreitung an ein Publikum auch in die Hände dieser Betroffenen gelegt werden soll.

…aus dem medizinischen Bereich

Eine zweite historische Grundlage hat die Fixierung auf personenbezogene Informationen in der spezifischen Konstruktion der informierten Einwilligung, wie sie von Oscar M. Ruebhausen und Orville G. Brim, Jr., aus der Medizinethik übernommen wurde.[19] Diese Arbeit, in der sich die Autoren unter anderem explizit auf die Ergebnisse des Nürnberger Ärzteprozesses bezogen, wurde in der zweiten Hälfte der 1960er und der ersten Hälfte der 1970er Jahre breit rezipiert, wenn es darum ging, welche Anforderungen an eine informierte Einwilligung zu stellen seien.

Der eigentliche Untersuchungsgegenstand der Arbeit war die Verhaltensforschung und die Frage, welche Informationen und welche Zusicherungen den Beforschten über die Erhebung, Speicherung und Verwendung der Informationen, die im Rahmen der Forschung anfallen, gegeben werden müssten.[20] Einer der wesentlichen Hintergründe ist natürlich, dass grundsätzlich davon ausgegangen werden kann, dass die Beforschten sich eher beforschen lassen und dabei wahrheitsgemäß antworten würden, wenn sie Vertrauen in die Integrität der Forscherinnen und Forscher und in die Vertraulichkeit ihrer gemachten Angaben haben.[21]

Auch hier geht es also wieder nicht darum, ob Entscheidungen über die Betroffenen getroffen werden und von wem, sondern – neben der Zweckbindung[22] – vor allem um die Frage einer eventuellen Weitergabe von Informationen aus dem Innenleben der Betroffenen, der private personality.

…von der Unterstellung eines fehlverstandenen Rationalismus

Eine dritte Ursache, die die Fixierung auf personenbezogene Informationen erklärt, liegt in einer weitverbreiteten Zuschreibung von Eigenschaften an einen bestimmten Akteur, der Entscheidungen über Menschen – und Dinge – trifft: die moderne Organisation.[23] In der Frühphase der modernen privacy- und Datenschutzdebatte werden solche Organisationen fast durchgängig als rationale Bürokratien im Weberschen Sinne verstanden, „die die Prozesse ihrer eigenen Entscheidungsfindung rational vorplanen, die dafür notwendigen Informationsverarbeitungsprozesse geeignet formalisieren und danach funktionieren wie ein Uhrwerk“.[24] Einer der wenigen, der offenlegt, wie sehr seine Konzeption von einer solchen zugeschriebenen, spezifischen Rationalität des Datenverarbeiters abhängig ist, ist Christoph Mallmann: „die Datenverarbeitung in der öffentlichen Verwaltung erfolgt zweckrational im Sinne Max Webers.“[25]

Dieser modernen Bürokratie wird also zugeschrieben, dass sie ihre rationalen Entscheidungen über Menschen in rationaler Weise treffen würde – und das heißt, auf der Basis von Informationen über diese Menschen,[26] und zwar möglichst vielen Informationen.[27] Sehr deutlich wird dies in Wilhelm Steinmüllers Annahme über das „unausgesprochene Ziel aller technokratisch ausgerichteten ADV“, der automationsunterstützten Datenverarbeitung: „Alle Daten über alle Betroffenen werden nur einmal erfaßt, einmal gespeichert, einmal gelöscht – »Minimierung der Datenmenge« –; alle Daten werden möglichst häufig verarbeitet und weitergegeben sowie möglichst vielen Benutzern zur Auswertung überlassen – »Maximierung der Datenflüsse und DV-Leistung« […]“[28]

Vor diesem Hintergrund wird dann verständlich, warum – trotz der schon seinerzeit, wenn auch selten, geäußerten Kritik[29] – es damals als zugleich notwendig wie hinreichend angesehen wurde, den „Informationshaushalt“ (Adalbert Podlech) der Organisationen zu regulieren,[30] um deren Produktion von Entscheidungen unter Kontrolle zu bringen. Es bleibt aber zu konstatieren, dass sich die Unterstellung, rationale Organisationen würden Entscheidungen über Menschen nur auf der Basis von personenbezogenen Informationen über diese Menschen treffen, inzwischen als nicht mehr haltbar herausgestellt hat.[31] Daher überrascht es durchaus, dass es bis heute – von einigen wenigen Ausführungen zum „Institutionaldatenschutz“[32] abgesehen – keine einzige privacy- oder Datenschutztheorie gibt, die ohne eine Anknüpfung an personenbezogene Informationen auskommt, obwohl diese (Selbst-)Beschränkung auf personenbezogene Informationen gerade nicht schon in der Analyse des Problems von Informationsmacht zwischen Organisation auf der einen und Individuen und Gruppen auf der anderen Seite selbst angelegt ist.[33]

Damit ist festzustellen, dass es zwar historische Zusammenhänge gibt, die die Fixierung auf personenbezogene Informationen erklären, um eine hinreichende Begründung handelt es sich dabei jedoch nicht. Wo sich in der Vergangenheit die Bezugnahme auf personenbezogene Informationen wissenschaftlich rechtfertigen musste, geschah dies ausschließlich in der Auseinandersetzung mit konkurrierenden Ansätzen wie etwa der Sphärentheorie oder der Privat-öffentlich-Dichotomie,[34] die zugleich jeweils nur eine Beschränkung des Anwendungsbereiches der jeweiligen privacy- und Datenschutztheorien auf Teilmengen von personenbezogenen Informationen forderten, etwa auf bestimmte Datenkategorien.

Folgen der Selbstbeschränkung auf personenbezogene Informationen

Die zweite zentrale Frage, der sich diese Arbeit annimmt, ist die nach den Folgen, die diese konzeptionelle Selbstbeschränkung für den Schutz von Betroffenen wie Alice in den oben beschriebenen und allen vergleichbaren Fällen hat.

Die offensichtliche Folge dieser Fixierung auf personenbezogene Informationen als Schutzobjekt entspricht dem, was Kuhn als Selbstisolierung von wissenschaftlichen Disziplinen oder Communities beschrieben hat: Das zugrunde liegende gesellschaftliche Problem – das Machtproblem und das Problem der Entscheidung über Menschen – kann schlicht nicht beschrieben werden „in terms of the conceptual and instrumental tools the [privacy, Einfügung des Autors] paradigm provides.“[35] Mit die-

ser Fixierung reproduziert sich zugleich – auf der gesellschaftlichen Ebene – die Schließung des Diskursraumes.[36]

Personenbezogene Informationen sind als Bezugspunkt und Schutzobjekt des Rechts aus informatischer, soziologischer wie rechtlicher Sicht ungeeignet, insoweit es für Organisationen möglich ist, individuelle Diskriminierung auch auf der Basis anonymer oder statistischer Informationen vorzunehmen. Das gilt gerade auch für strukturell vermachtete Verhältnisse wie die zwischen Organisationen und ihrem Klientel. Sowohl aus der Außenperspektive wie aus der Perspektive von Alice ist es gleich, ob Google – oder irgendeine andere (informations-) mächtige Organisation – Entscheidungen über sie auf der Basis von Informationen über sie oder über andere Menschen trifft. Auch kann Alice – sowohl nach der derzeitigen Datenschutzrechtslage wie nach allen privacy-Theorien – nicht einmal feststellen, auf welcher Basis Google über sie entscheidet, solange es sich dabei nicht um personenbezogene Informationen über sie selbst handelt, denn Google ist ihr darüber nicht begründungspflichtig. Statt dessen perpetuiert und zementiert sich damit Googles Informationsmacht über Alice.

Die Entscheidung, Alice – und alle anderen Betroffenen – im vermachteten Verhältnis zu Organisationen nur dann zu schützen, wenn die Organisation ihre Macht unter Verwendung personenbezogener Informationen über Alice ausübt, ist sowohl arbiträr wie am eigentlichen Problem vorbeigehend.[37] Alice wird der Macht der Organisation gerade immer dann schutzlos ausgeliefert, wenn es der Organisation gelingt, ihre Machtbasis, nämlich Informationen, erfolgreich zu tarnen: Eine jede Theorie, die personenbezogene Informationen und deren Erhebung, Speicherung, Verarbeitung und Verwendung falsch als das Problem selbst ausweist, erklärt damit zugleich die Erhebung, Speicherung, Verarbeitung und Verwendung anderer als personenbezogener Informationen für unproblematisch. Die Nicht-Verarbeitung personenbezogener Informationen, die (Selbst-)„Beschränkung" von Organisationen auf die Verarbeitung anonymer oder anonymisierter Informationen, die Möglichkeiten zum „Selbstdatenschutz" – dies alles sind nur Placebos zur Beruhigung der Betroffenen[38] und zur Sicherstellung der gesellschaftlichen Akzeptanz einer „universellen Verdatung aller Lebensbereiche".[39] Es ist darum auch kein Wunder, wenn der Schutz von Betroffenen vor der „überlegen standardisierenden Strukturierungsmacht von Organisationen",[40] den privacy- und Datenschutztheorien zu verfolgen vorgeben,[41] inzwischen häufig nicht mehr als privacy- oder Datenschutzproblem, sondern als Verbraucher_innenschutz- oder Kartellrechtsproblem betrachtet wird – und betrachtet werden muss, weil sich privacy- und Datenschutztheorien einer Auseinandersetzung damit verweigern.

Personenbezogene Entscheidungen als passenderer Anknüpfungspunkt

Die dritte Frage, die sich in diesem Zusammenhang stellt, ist nun offensichtlich: Welcher Anknüpfungspunkt ist besser geeignet als das Konzept der personenbezogenen Informationen, um in vermachteten Informationsbeziehungen wie in den oben beschriebenen und allen vergleichbaren Fällen den Schutz von Betroffenen wie Alice sicherzustellen? Aus dem Vorstehenden lässt sich bereits ersehen, wie dieser Ansatz aussehen kann, um den Datenschutz und das Datenschutzrecht vom Kopf auf die Füße zu stellen.

Sicher ist, dass eine Datenschutztheorie für sich in Anspruch nehmen sollte, die strukturellen Machtasymmetrien, die mit der und durch die Industrialisierung der gesellschaftlichen Informationsverarbeitung erzeugt, verstärkt oder verfestigt werden,[42] als solche zu problematisieren, unabhängig davon, ob sich die verarbeiteten Informationen auf Individuen, Gruppen, Organisationen, Sachen oder selbst Konzepte beziehen. Aber auch wenn sie das nicht versucht, muss sie zumindest die Klasse von Problemen adressieren, die entstehen, wenn in solchen vermachteten Verhältnissen sozial, politisch und ökonomisch mächtige Akteure Entscheidungen über Menschen treffen und diese Akteure dann in der Lage sind, diese Entscheidungen den Menschen zu oktroyieren. Die individuelle Betroffenheit, die offensichtlich in der von der liberalen Ideologie geprägten Vorstellung der bürgerlichen Gesellschaft nachgewiesen werden muss, damit ein gesellschaftliches Problem politisch wie rechtlich adressierbar wird – wenn auch eben nur in der Form einer individuellen Betroffenheit –, entsteht gerade aus sozial relevanten personenbezogenen Entscheidungen in strukturell vermachteten Informationsbeziehungen. Über diesen Anknüpfungspunkt der personenbezogenen Entscheidung wären dann auch alle Informationen, die zur Grundlage dieser Entscheidung gemacht worden sind oder gemacht werden sollen, und nicht nur die personenbezogenen, rechtlich adressierbar.[43]

Mit einer derart gestalteten Anknüpfung an automationsgestützte personenbezogene Entscheidungen in strukturell vermachteten Verhältnissen lassen sich nicht nur die historischen Fehlübernahmen aus Gegenstandsbereichen, die mit Entscheidungsfindung nichts zu tun haben, korrigieren, sondern es erlaubt auch, ein weiteres – weitgehend in Vergessenheit geratenes – Problem zu adressieren: Schon die Diskussionen in den privacy-Anhörungen in beiden Kammern des United States Congress in den 1960er Jahren zeigten, dass die Regulierung von Nutzungen – und dazu gehören auch Entscheidungen – allein nicht ausreicht.[44] Der Grund dafür ist offenkundig: Die Entscheidungen sind selbst „Produkt" der Informationen und ihrer Verarbeitung, wobei die Informationen wiederum „Produkt" der zugrunde gelegten Modellannahmen sind.[45] Daraus folgt dann aber zwingend, dass eine Anknüpfung an automationsgestützte personenbezogene Entscheidungen gerade nicht zu einer erneuten Selbstbeschränkung führen darf – hier nun als Selbstbeschränkung auf die Entscheidung –, sondern die Produktion der Entscheidung und deren Bedingungen zum Gegenstand von Theorie und Regulierung machen muss.

Wenn also das Ziel des Datenschutzes nicht einfach sein soll, mit überkommenen Regelungsinstrumenten individuelle Befindlichkeiten zu schützen, sondern die Freiheitsräume – als die Bedingungen der Möglichkeit zur Freiheitsausübung – von strukturell und informationell Schwächeren unter den Bedingungen der Industrialisierung der gesellschaftlichen Informationsverar-

beitung und gegen die überlegen standardisierende Strukturierungsmacht von Organisationen zu schützen, indem die Modellifizierungs- und Entscheidungsmacht von Organisationen mit ihren Folgen für Individuen und Gesellschaft, für Rechtsstaat, Sozialstaat und Demokratie und für die Freiheitsversprechen der bürgerlichen Gesellschaft wirksam beschränkt wird, dann gilt es, dafür die passenden Konzepte, Anknüpfungspunkte und Instrumente auszuwählen. Dazu muss eine Umstellung vorgenommen werden, denn nicht einfach die personenbezogenen Informationen, sondern die personenbezogenen Entscheidungen sind es, die durch das Datenschutzrecht unter Bedingungen zu stellen sind. Das gilt es zum Thema einer informierten Datenschutzdebatte zu machen, bevor das Problem – dann wiederum nur einseitig – als Verbraucher_innenschutz- oder Kartellrechtsproblem endet.

1 Siehe dazu Walter Bryce Gallie. „Essentially Contested Concepts“. In: Proceedings of the Aristotelian Society. New Series 56 (1956), S. 167–198. Ich bedanke mich bei Michael Plöse und Martin Rost für die kritische Durchsicht dieses Beitrags und die sehr produktiven Diskussionen zu Datenschutztheorie und Datenschutzrecht.

2 Auch an dieser Stelle gibt es genug Raum für Streit, etwa zum Begriff und zum zugrunde gelegten Informationskonzept, zur Frage, welche Rolle genau personenbezogene Informationen in diesem Zusammenhang spielen – etwa ob sie Schutzgut oder nur rechtlicher Anknüpfungspunkt sind –, ob alle Informationen oder nur „private“ – im Gegensatz zu „öffentlichen“ – oder nur „sensitive“ – im Gegensatz zu „nicht-sensitiven“ – eingeschlossen werden und ob sich „personenbezogen“ nur auf Menschen oder auch auf Gruppen oder Organisationen – in der Sprache des Rechts: juristische Personen – bezieht.

3 Siehe § 3 Abs. 1 BDSG. Über den Bezeichner „Daten“ ist schon genug geschrieben worden, es handelt sich aber klar um einen Informationsbegriff, siehe Jörg Pohle. „Die immer noch aktuellen Grundfragen des Datenschutzes“. In: Wovon – für wen – wozu. Systemdenken wider die Diktatur der Daten. Wilhelm Steinmüller zum Gedächtnis. Hrsg. von Hansjürgen Garstka und Wolfgang Coy. Humboldt-Universität zu Berlin, Hermann von Helmholtz-Zentrum für Kulturtechnik. Berlin, 2014, S. 45–58. URL: http://nbn-resolving.de/urn:nbn:de:kobv:11-100217316, S. 49 f.

4 Google ist eine „Weltvermessungsfirma“ (Martin Rost), ökonomisch allerdings in erster Linie eine Werbefirma mit angeschlossener Suchmaschine.

5 Das Management von Google trifft allerdings durchaus politisch relevante Entscheidungen, die dann als Technik, als Basis der Industrialisierung, auskristallisieren. Für diese saubere Trennung zwischen den unterschiedlichen Entscheidungsebenen, die sich auch in unterschiedlichen Folgen niederschlagen, danke ich Martin Rost.

6 Ulrich Dammann in Spiros Simitis, Hrsg. Bundesdatenschutzgesetz. 7. Aufl. Baden-Baden: Nomos Verlagsgesellschaft, 2011, § 3 Rn. 198.

7 Das gilt selbst für Konstrukte wie dezisionale Privatheit, siehe Beate Rössler. Der Wert des Privaten. Frankfurt am Main: Suhrkamp Verlag, 2001, S. 18, 25, 144 ff. wenn diese sich nicht schon auf jede von beliebigen Anderen beeinflusste Entscheidungsgrundlagen beziehen sollen, sondern sich – wie bei Rössler – auf intentionale Beeinflussung von Entscheidungen beschränken. Siehe dazu etwa die Verwendung des Begriffs „einmischen“, S. 148.

8 Siehe § 13 Abs. 6 TMG, siehe dazu auch die Diskussion zu dem von Marit Hansen angesprochenen Fall in Jörg Pohle und Andrea Knaut, Hrsg. Fundationes I: Geschichte und Theorie des Datenschutzes. Münster: Monsenstein und Vannerdat, 2014, S. 218, Rn. 35 und S. 225, Rn. 53 ff.

9 Einen ersten Schritt zur Überwindung dieser Beschränkung geht das Standard-Datenschutzmodell, siehe grundlegend Martin Rost. „Standardisierte Datenschutzmodellierung“. In: Datenschutz und Datensicherheit 36.6 (2012), S. 433–438, das personenbezogene Verfahren zugrunde legt. Damit soll bereits auf das Prozessieren von Daten, gleich welchen Ursprungs, auf Seiten von Organisationen verwiesen werden, wenn sie nur auf Personen bezogen werden. Siehe aber auch die eingeschränktere Definition im SDM-Handbuch, die immer noch auf dem Konzept der personenbezogenen Daten aufsetzt, Das Standard-Datenschutzmodell: Konzept zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, 2015. URL: https://www.datenschutz-mv.de/datenschutz/sdm/SDM-Handbuch_V09a.pdf, S. 7, 29, und zugleich die darüber hinausreichenden Beispiele, etwa S. 21 f.

10 Dieser Problembereich, also etwa die mögliche Diskriminierung auch anonymisierter Personen aufgrund statistischer Informationen, mag inzwischen durchaus diskutiert werden, siehe zuletzt Alexander Roßnagel und Maxi Nebel. „(Verlorene) Selbstbestimmung im Datenmeer: Privatheit im Zeitalter von Big Data“. In: Datenschutz und Datensicherheit (2015), S. 455–459, aber diese Diskussion führte bislang an keiner Stelle zu der Erkenntnis, dass das Problem in der arbiträren Anknüpfung an personenbezogene Informationen liegt.

11 Siehe Hans-Heinrich Maass. Information und Geheimnis im Zivilrecht. Stuttgart: Ferdinand Enke Verlag, 1970, S. 15.

12 Samuel D. Warren und Louis D. Brandeis. „The Right to Privacy“. In: Harvard Law Review (1890), S. 193– 220.

13 Josef Kohler. Das Autorrecht. Jena: Verlag Gustav Fischer, 1880.

14 James Whitmans Arbeit, in der es um das Verhältnis zwischen den europäischen und amerikanischen Ansätzen geht, kann nicht wirklich als wissenschaftlich durchgehen, und das nicht nur weil er aus unerfindlichen Gründen versucht, Warren und Brandeis Arbeit mit der Otto von Gierkes zu vergleichen, siehe James Q. Whitman. „The Two Western Cultures of Privacy: Dignity versus Liberty“. In: The Yale Law Journal 113.6 (2004), S. 1151–1221. Eine umfassende Untersuchung steht also noch immer aus.

15 Siehe Warren und Brandeis, „The Right to Privacy“, S. 197 f.

16 Kohler, Das Autorrecht, S. 137.

17 Warren und Brandeis, „The Right to Privacy“, S. 198.

18 Warren und Brandeis, „The Right to Privacy“, S. 195. Bei Kohler heißt es noch „das Heiligthum des geistigen Innenlebens“, siehe Kohler, Das Autorrecht, S. 142.

19 Siehe Oscar M. Ruebhausen und Orville G. Brim Jr. „Privacy and Behavioral Research“. In: Columbia Law Review 65.7 (1965), S. 1184–1211.

20 Siehe Ruebhausen und Brim, „Privacy and Behavioral Research“, S.1196 f. „first, the degree of individual consent that exists and, second, the degree of confidentiality that is maintained. The former concerns the conditions under which information is obtained from a person, the latter, the conditions under which the information is used.“

21 Dieser sehr pragmatische Grund für die Gewährleistung von privacy wird explizit angesprochen, siehe Ruebhausen und Brim, „Privacy and Behavioral Research“, S. 1198.

22 Zum Einfluss dieser Arbeit auf die historische Konstruktion des Zweckbindungsgrundsatzes, siehe Jörg Pohle. „Zweck-

bindung revisited“. In: Datenschutz Nachrichten 38.3 (2015), S. 141–145, S. 141.

23 Das nachfolgende gilt natürlich nur für Theorieansätze, die den Angreifer nicht in anderen Menschen verorten, sondern in Organisationen. Die meisten privacy-, Privatheits- und Privatsphäretheorien, aber auch einige der Theorien zum Datenschutz sind hinsichtlich der Angreifer personenfixiert.

24 Pohle, „Die immer noch aktuellen Grundfragen des Datenschutzes“, S. 49. Siehe dazu etwa die Darstellung der Organisationen bei Wilhelm Steinmüller u. a. Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. VI/3826, Anlage 1. 1971, S. 49, Ernst Benda. „Privatsphäre und „Persönlichkeitsprofil““. In: Menschenwürde und freiheitliche Rechtsordnung. Festschrift für Willi Geiger zum 65. Geburtstag. Hrsg. von Gerhard Leibholz u. a. Tübingen: J. C. B. Mohr (Paul Siebeck), 1974, S. 23–44, S. 27, Adalbert Podlech. „Aufgaben und Problematik des Datenschutzes“. In: Datenverarbeitung im Recht 5 (1976), S. 23–39, S. 25 oder James B. Rule u. a. The Politics of Privacy. New York: Elsevier, 1980, S. 25 ff.

25 Christoph Mallmann. Datenschutz in Verwaltungs-Informationssystemen. München, Wien: R. Oldenbourg Verlag, 1976, S. 32 mit Verweis auf Niklas Luhmann. „Zweck – Herrschaft – System. Grundbegriffe und Prämissen Max Webers“. In: Der Staat 3.2 (1964), S. 129–158 und Niklas Luhmann. Funktionen und Folgen formaler Organisation. Berlin: Duncker & Humblot, 1964. Hervorhebung im Original.

26 So explizit James B. Rule. Private Lives and Public Surveillance. London: Allen Lane, 1973, S. 29.

27 Siehe M. G. Stone und Malcolm Warner. „Politics, Privacy, and Computers“. In: The Political Quarterly 40.3 (1969), S. 256–267. S. 258.

28 Wilhelm Steinmüller. „Datenschutz als Teilaspekt gesellschaftlicher Informationskontrolle“. In: Datenschutz und Datensicherung. Hrsg. von Gerhard Löchner und Wilhelm Steinmüller. Karlsruhe: C. F. Müller Verlag, 1975, S. 35–95, S. 49.

29 Siehe etwa Paul J. Müller. „Informationsflüsse und Informationshaushalte“. In: Informationsrecht und Informationspolitik. Hrsg. von Wilhelm Steinmüller. München, Wien: Oldenbourg Verlag, 1976, S. 95–109, S. 96 f.

30 Dass es sich dabei nicht allein um eine auf die Bundesrepublik beschränkte Debatte handelte, zeigen die Ausführungen dazu bei Rule, Private Lives and Public Surveillance, S. 285.

31 Siehe etwa die Darstellung der Übertragung statistischer Informationen und deren Anwendung auf Individuen bei Eike Kühl. „Zeig uns dein Smartphone und wir leihen dir Geld“. In: Zeit Online (2015). URL: http://www.zeit.de/digital/internet/2015-12/kreditwuerdigkeit-scoring-smartphone-big-data.

32 Siehe dazu die thematische Kurzübersicht bei Steinmüller u. a., Grundfragen des Datenschutzes, S. 34.

33 Siehe etwa die Darstellung bei Klaus Lenk. „Datenschutz in der öffentlichen Verwaltung“. In: Datenschutz. Hrsg. von Wolfgang Kilian, Klaus Lenk und Wilhelm Steinmüller. Frankfurt am Main: Athenäum-Verlag, 1973, S. 15–50, S. 21 ff. Dabei ist jedoch durchaus zu beachten, dass der Begriff des Personenbezugs damals eher weit verstanden wurde, wie sich etwa an der Argumentation zur Relativität des Personenbezugs von Informationen bei Wilhelm Steinmüller. „Datenschutzrechtliche Anforderungen an die Organisation von Informationszentren“. In: Internationale Fachtagung: Informationszentren in Wirtschaft und Verwaltung. Hrsg. von P. Schmitz. Berlin, Heidelberg, New York: Springer, 1974, S. 187–205, S. 193 zeigt.

34 Siehe zu dieser Auseinandersetzung Jörg Pohle. „Die kategoriale Trennung zwischen »öffentlich« und »privat« ist durch die Digitalisierung aller Lebensbereiche überholt – Über einen bislang ignorierten Paradigmenwechsel in der Datenschutzdebatte“. In: »Worüber reden wir eigentlich?« Festgabe für Rosemarie Will. Hrsg. von Michael Plöse u. a. Humanistische Union. Berlin, i.E.

35 Thomas S. Kuhn. The Structure of Scientific Revolutions. 3. Aufl. Chicago, London: The University of Chicago Press, 1996, S. 37.

36 Siehe dazu Herbert Marcuse. One-Dimensional Man. Studies in the ideology of advanced industrial society. Reprint der 2. Auflage von 1991. London, New York: Routledge, 2002, S. 87 ff.

37 Bezeichnenderweise gibt es selbst in dem sehr umfassenden BDSG-Kommentar von Simitis an keiner Stelle eine Begründung für diese Entscheidung. Statt dessen wird einfach erklärt, Ziel sei „einzig und allein den Schutz vor den Folgen sicherzustellen, die eine Verarbeitung personenbezogener Angaben für die jeweils davon Betroffenen haben kann“, siehe Simitis, Bundesdatenschutzgesetz, Einleitung, Rn. 2.

38 Und sie sind zugleich sehr wirkmächtige Selbstbeschränkungen in der Gestaltung von Technik, siehe Jörg Pohle. „Das Scheitern von Datenschutz by Design: Eine kurze Geschichte des Versagens“. In: FIfF Kommunikation 32 (2015), S. 41–44, S. 43.

39 Wilhelm Steinmüller. „Die Zweite industrielle Revolution hat eben begonnen – Über die Technisierung der geistigen Arbeit“. In: Kursbuch 66 (1981), S. 152–188.

40 Wolfgang Zimmermann. „Privatsphäre. Aufruf zur Konstruktion einer realitätsbezogenen Bildwelt“. In: Fundationes I: Geschichte und Theorie des Datenschutzes. Hrsg. von Jörg Pohle und Andrea Knaut. Münster: Monsenstein und Vannerdat, 2014, S. 45–63, Rn. 35.

41 Siehe statt vieler zum Ziel des Datenschutzrechts als Normierung von „Datenmacht“ zur Sicherstellung ihrer Beschränkbarkeit und Kontrolle Kai von Lewinski. „Geschichte des Datenschutzrechts von 1600 bis 1977“. In: Freiheit – Sicherheit – Öffentlichkeit. Hrsg. von Felix Arndt. 48. Assistententagung Öffentliches Recht. Nomos Verlagsgesellschaft, 2009, S. 196–220, S. 200.

42 Siehe dazu Jörg Pohle. „Transparenz und Berechenbarkeit vs. Autonomie- und Kontrollverlust: Die Industrialisierung der gesellschaftlichen Informationsverarbeitung und ihre Folgen“. In: Mediale Kontrolle unter Beobachtung (i.E.). Dieser Fokus auf die Gesellschaft ist jedoch keineswegs neu. So werden schon Ende der 1970er Jahre „Verhinderung des Mißbrauchs personenbezogener Daten“ und „Gesamtheit der Maßnahmen zur Ermöglichung und Erhaltung sozialer Verhaltensräume für Individuen und Gruppen unter den Bedingungen moderner Informations- und Kommunikationssysteme“ als die beiden konzeptionellen Extrempunkte in der Datenschutzdebatte identifiziert, siehe Klaus Dette. „Einführung in das Kolloquium und Zusammenfassung der Ergebnisse“. In: Zweiweg-Kabelfernsehen und Datenschutz. Hrsg. von Klaus Dette, Rolf Kreibich und Wilhelm Steinmüller. Institut für Zukunftsforschung. München: Minerva Publikation, 1979, S. 3–13, S. 8.

43 Siehe schon Pohle, „Zweckbindung revisited“, S. 143.

44 Siehe schon Arthur Raphael Miller. „Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society“. In: Michigan Law Review 67.6 (1969), S. 1089–1246. S. 1221 i. V. m. S. 1119 f.

45 Ausführlich dazu Pohle, „Transparenz und Berechenbarkeit vs. Autonomie- und Kontrollverlust: Die Industrialisierung der gesellschaftlichen Informationsverarbeitung und ihre Folgen“.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Kanzleramt will BND besser kontrollieren

Als Konsequenz aus dem NSA-Skandal will das Kanzleramt den Bundesnachrichtendienst (BND), den deutschen Auslandsgeheimdienst, an eine kürzere Leine nehmen und dem Bundestag ein schärferes Kontrollrecht geben. Die Zusammenarbeit mit ausländischen Partnern wie dem US-Dienst National Security Agency (NSA) soll strengeren Regeln unterworfen werden. Die Rolle der Regierungszentrale als Genehmigungs- und Kontrollinstanz soll verstärkt, Wirtschaftsspionage ausgeschlossen werden. Der BND war im Zusammenhang mit der NSA-Affäre u. a. in die Kritik geraten, weil er für die NSA lange Zeit unzulässige Suchbegriffe eingesetzt hatte. Diese sollen nach BND-Angaben mittlerweile aussortiert sein. Auch BND-eigene sogenannte Selektoren zur Spionage im weltweiten Datenstrom sollen gegen das Auftragsprofil des Dienstes verstoßen haben. Der BND hatte immer wieder betont, etwa keine Wirtschaftsspionage zu betreiben.

Im mehr als 30-seitigen Entwurf des Kanzleramts heißt es, Ziel des Gesetzes sei es insbesondere, Rechtsklarheit bei der Fernmeldeaufklärung von AusländerInnen im Ausland herzustellen, die der Auslandsnachrichtendienst von deutschem Boden aus betreibt. Es gehe darum, „dadurch das Vertrauen in die Tätigkeit des BND zu stärken“ und die Rechtssicherheit für dessen MitarbeiterInnen zu erhöhen. Das Kanzleramt stellt sich mit dem Entwurf weiterhin hinter den Auftrag des BND zur Aufklärung von für die Außen- und Sicherheitspolitik bedeutsamen Themen, etwa im Kampf gegen den Terror, die Verbreitung von Massenvernichtungswaffen, die organisierte Kriminalität und die Aufklärung der politischen Lage in bestimmten Ländern.

Der Einsatz der umstrittenen Suchbegriffe soll nach dem Entwurf eingegrenzt werden. Es dürften nur Begriffe verwendet werden, die „im Einklang mit den außen- und sicherheitspolitischen Interessen“ Deutschlands stünden. An dieser Selbstverständlichkeit hatte es Zweifel gegeben. Dem Dienst war vorgeworfen worden, unrechtmäßig auch europäische Behörden, diplomatische Einrichtungen und in Einzelfällen verbotenerweise sogar deutsche Staatsbürger im Ausland ausspioniert zu haben. Im Entwurf heißt es: „Suchbegriffe, die zur gezielten Erfassung von Einrichtungen der Europäischen Union, öffentlichen Stellen ihrer Mitgliedstaaten oder von Unionsbürgern führen, dürfen durch den Bundesnachrichtendienst nur verwendet werden, wenn dies zur rechtzeitigen Erkennung und Begegnung von Gefahren für bedeutende Rechtsgüter notwendig ist.“

Suchbegriffe dürften in diesem Zusammenhang „nur nach Anordnung durch den Behördenleiter oder seinen Stellvertreter verwendet werden, wenn dies zur Aufklärung eines Vorgangs mit besonderer Auftragsrelevanz erforderlich ist“. Das Kanzleramt sei über diese Anordnungen zu unterrichten. Zudem soll das Kanzleramt auf Antrag des BND-Präsidenten oder seines Stellvertreters entscheiden, in welchen Telekommunikationsnetzen jeweils spioniert werden darf.

Das Kanzleramt soll demnach monatlich eine noch zu bestimmende Kontrollkommission über diese Anordnungen unterrichten – und zwar vor deren Vollzug. Dieses Gremium solle „Zulässigkeit und Notwendigkeit der Anordnung“ prüfen. Eine Vorab-Unterrichtung könne unterbleiben, wenn die Gefahr bestehe, dass dadurch „das Ziel der Maßnahme vereitelt oder wesentlich erschwert wird“. Im Gespräch war 2015 zudem die Einsetzung eines ständigen Bevollmächtigten zur Verbesserung der parlamentarischen Kontrolle. Gemäß dem Gesetzentwurf müssten durch das neu einzuführende Antragsverfahren im Kanzleramt drei und beim BND voraussichtlich zwölf zusätzliche Planstellen geschaffen werden. Die damit verbundenen jährlichen zusätzlichen Personalkosten werden insgesamt auf knapp zwei Millionen Euro beziffert.

Der Entwurf ist noch nicht in der Koalition abgestimmt und eine erste Grundlage für weitere Diskussionen. Der innenpolitische Sprecher der Unionsfraktion, Stephan Mayer (CSU), erklärte: „Wir werden sehr genau schauen müssen, ob der jetzige Entwurf nicht zu weit geht, wir dürfen den BND nicht entmannen“. Die SPD soll den Vorschlägen des Kanzleramts weitgehend zustimmen. In einem Punkt verlangt sie eine Nachbesserung: Die Regierung will die neuen Regeln nur gelten lassen, wenn die Abhöroperationen aus Deutschland heraus stattfinden oder wenn sog. Transitverkehre – etwa am Internetknoten in Frankfurt – auf deutschem Boden abgefangen werden. Die SPD fordert dagegen eine weltweite Gültigkeit bei den Abhörpraktiken (Kanzleramt will BND an kürzere Leine nehmen, www.n24.de 19.01.2016; Leyendecker/Mascolo, Kanzleramt will BND beim Abhören bremsen, SZ 19.01.2016, 6).

Bund

Diskussion um Leitung des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Am 11.12.2015 wurde der bisherige Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) Michael Hange von Bundesinnenminister Thomas de Maizière wegen Erreichen der Altersgrenze in den Ruhestand verabschiedet. Der Diplom-Mathematiker und Kryptologe Hange war 1977 in die Bundesverwaltung eingetreten und mit der Gründung des BSI im Jahre 1991 in

die Sicherheitsbehörde gewechselt, wo er die Abteilung leitete, die das Konzept für ein IT-Grundschutzhandbuch entwickelte. Von 1994 bis 2009 war Hange Vizepräsident des BSI, von 2009 bis zum November 2015 Präsident der obersten deutschen Sicherheitsbehörde. Seit 2011 war er zudem Sprecher des Nationalen Cyber-Abwehrzentrums. Hange war ein Garant dafür, dass das BSI mit seinen 600 Beschäftigten insbesondere aus den Bereichen Informatik und Mathematik, nachdem es aus dem Bundesnachrichtendienst und damit aus einem Geheimdienst herausgelöst worden war, eine eigenständige zivile Funktion im Interesse der Datensicherheit übernahm. Hange suchte dabei auch den Austausch und die Kooperation mit den Datenschutzbeauftragten des Bundes und der Länder, zu deren Tätigkeit es Überschneidungen mit dem BSI gibt. Eine enge Zusammenarbeit zwischen dem unabhängigen Datenschutz und dem beim Bundesinnenministerium angegliederten BSI ist von großer Bedeutung für eine Abstimmung zwischen IT-Sicherheit und digitalem Grundrechtsschutz.

Nachfolger Hanges soll nach dem Willen des Bundesinnenministeriums (BMI) der 46-jährige Betriebswirt Arne Schönbohm werden. Dieser ist Sohn des CDU-Innenpolitikers und Generalleutnants a. D. Jörg Schönbohm. Arne Schönbohn ist bisher Vorstandsvorsitzender der BuCET Shared Services AG (BSS AG), die er mit seinem Bruder Hendrik leitet, und Präsident des von ihm mit gegründeten Cyber-Sicherheitsrates Deutschland. Mit dieser bewusst gewollten „externen Lösung“ soll nach Darstellung des BMI der Kontakt zwischen der Wirtschaft und dem BSI intensiviert werden.

Die Ansage, Schönbohm zum neuen Leiter des BSI zu machen, ist in der Behörde selbst auf Irritationen gestoßen. Es war damit gerechnet worden, dass Vizepräsident Andreas Könen die Leitung übernehmen würde, so wie sie Hange von Udo Helmbrecht übernahm, als dieser zur europäischen Sicherheitsagentur ENISA wechselte. Könen hatte schon zur Amtszeit von Hange das BSI in der Öffentlichkeit oft vertreten. Er zeichnet sich durch hohe fachliche Kompetenz und durch eine neutrale Amtsführung aus.

Der FDP-Politiker Schönbohm arbeitete zunächst als Lobbyist für den Rüstungskonzern EADS Defence and Space. Er wurde mit Überlegungen bekannt, das Funksystem der Sicherheitsbehörden mit dem (von EADS gelieferten) Funk-System der Bundeswehr zu integrieren, um besser in der Terror-Abwehr aufgestellt zu sein. Er zeichnete für das Tetra-Desaster (BOSNet) mitverantwortlich. Später gründete er unter dem Eindruck der Stuxnet-Attacke im August 2012 den Cyber-Sicherheitsrat Deutschland e.V., der große und mittelständische Unternehmen in Sachen Cyber-Sicherheit berät. Nach eigenen Angaben ist er zudem Mitglied im „Förderkreis Heer“, einem Lobbyverband der Rüstungswirtschaft, und in der „Deutschen Gesellschaft für Wehrtechnik“, in dem sich Rüstungsfirmen und Abgeordnete vernetzen. Gemäß einem von ihm 2011 verfassten Ratgeber für „positive Lebensphilosophie“ mit dem Titel „Erfolgreicher Weg“ wollte er als Kind Bundeskanzler werden. Zitat: „Ich gelte jetzt als einer der renommierten Sicherheitsberater Deutschlands. Ich möchte gern DER renommierte Sicherheitsberater Deutschlands und Europas werden.“ Zuletzt hatte er sich dafür stark gemacht, dass die Telematik-Infrastruktur der elektronischen Gesundheitskarte für externe Anbieter geöffnet wird.

Der Verein „Cybersicherheitsrat Deutschland e. V.“, dessen Vorsitzender Schönbohm seit Sommer 2012 ist, vertritt angeblich die Interessen von nahezu 2 Millionen Beschäftigten aus der Wirtschaft. Die Namenswahl des privaten Vereins wurde von offizieller Seite als Provokation empfunden, da 17 Monate zuvor die Bundesregierung unter Federführung des BMI einen „Nationalen Sicherheitsrat“ ins Leben gerufen hatte. Der Verein hat sich zudem die Internetdomain „cybersicherheitsrat.de“ gesichert und wirbt für sich mit einem schwarz-rot-goldenen Vereinslogo. Auf der Mitgliederliste des von Schönbohm geleiteten Cyber-Sicherheitsrates stehen neben TÜV, Commerzbank und einer Online-Apotheke vor allem Firmen wie IBM, die Waffensparte von EADS und IT-Sicherheitsfirmen wie Kaspersky. Vertreten wird also die Branche, deren Produkte das BSI prüft und zertifiziert.

Die von Schönbohm geleitete BSS AG wirbt für sich, dass sie Unternehmen und Behörden in den Bereichen Digitalisierung, Cyber-Sicherheit und Datenschutz berate. Tatsächlich ist Schönbohm im Bereich Datenschutz bis heute überhaupt nicht öffentlich in Erscheinung getreten. Das BMI hatte angekündigt, dass Schönbohm im Fall einer Ernennung als BSI-Präsident die Anteile an seiner Beratungsfirma verkaufen und sich aus dem Cyber-Sicherheitsrat zurückziehen werde.

Schönbohm hatte in einem Interview 2014 gefordert, einen direkt im Kanzleramt angesiedelten „Cyber-Zar“ nach amerikanischen Vorbild einzuführen. Für das Bundesinnenministerium ist Schönbohm ein „kritischer Geist“, der auch öffentlich eine andere Meinung als die Behörde vertreten habe. Aus Schönbohms Sicht ist Deutschland zu schlecht gegen Online-Bedrohungen gerüstet. Er war einer der lautesten, nicht der qualifiziertesten Gegner des im Sommer 2015 verabschiedeten IT-Sicherheitsgesetzes, das nun vom BSI umgesetzt werden muss. So äußerte er gegenüber der Presse: „Eigentlich ist das Bundesinnenministerium mit seinem Kampf gegen Cyberattacken gescheitert.“

Der netzpolitische Sprecher der Grünen, Konstantin von Notz sieht in Schönbohm keinen „IT-Experten“, sondern einen „IT-Lobbyisten“: „Man wird das Gefühl nicht los, dass sich das Bundesinnenministerium nicht angeschaut hat, wen man da eigentlich an die Spitze setzen will“. Der Cyber-Sicherheitsrat sei vor allem ein „Visitenkarten-Institut“ mit wenig Substanz. Auch der netzpolitische Sprecher der SPD-Fraktion, Lars Klingbeil, kritisierte die Personalvorauswahl des BMI: „Es ist nicht unproblematisch, wenn jemand als Verbandsvertreter das IT-Sicherheitsgesetz verhindern wollte und nun wenige Wochen später als Präsident des BSI die konkrete Umsetzung verantworten soll.“

Kritik an der Benennung Schönbohms äußerte auch „Netzpolitik.org“. Danach sei hier „Kompetenz kein Einstellungskriterium“. Schönbohm habe sich mit „Cyber-Bullshitting“, hohlem Gerede mit technologisch klingenden Phrasen, hervorgetan. Die Sprecherin des Chaos Computer Clubs (CCC) Konstanze Kurz nannte Schönbohm einen „Cyberclown“, der Regierungen schon häufiger teure,

aber überflüssige IT-Lösungen angedreht habe. Der IT-Experte Sandro Gayken ergänzte: „In seinen Interviews und seinem Buch käut Schönbohm vorwiegend die Thesen anderer wider; seine technische Kompetenz geht gegen Null“ (Brühl, Vorwürfe gegen designierten BSI-Chef: „Cyber-Bullshitting“ und Lobbyismus, http://www.sueddeutsche.de 22.12.2015, Borchers, BSI-Chef Hange ist im Ruhestand, www.heise.de 14.12.2015; Rosenbach/Schindler, „Eigentlich gescheitert“, Der Spiegel 53/2015, 38; „Im Kampf gegen Cyberattacken gescheitert“, www.welt.de 11.10.2014, Kurz, Neuer BSI-Präsident vorgeschlagen: Kompetenz kein Einstellungskriterium, www.netzpolitik.org 14.12.2015).

Nach Redaktionsschluss beschloss das Bundeskabinett am 17.02., Arne Schönbohm zum BSI-Chef zu machen. Bundesinnenminister Thomas de Maizière ernannte ihn noch am gleichen Tag. Am darauf folgenden Tag trat er sein Amt an.

Bund

Datenschutz-Verbandsklage beschlossen

Mit den Stimmen der Koalition hat der Deutsche Bundestag am 15.12.2015 ein Gesetz für neue „verbraucherschützende Vorschriften des Datenschutzrechts“ verabschiedet, mit dem Datenschutz zivilrechtlich einfacher durchsetzbar werden soll. Verbraucherverbände und Wirtschafts- sowie Wettbewerbskammern sollen damit künftig das Recht erhalten, gegen Datenschutzverstöße von Firmen zu klagen oder diese abzumahnen. Für das Vorhaben stimmten die Regierungsfraktionen von CDU/CSU und SPD. Linke und Grüne enthielten sich.

Bislang können Verbraucherschützer nur eingeschränkt stellvertretend für Betroffene von Datenmissbrauch tätig werden, wenn es etwa um unzulässige Verträge oder Allgemeine Geschäftsbedingungen (AGB) geht. Sammelt eine Firma ohne ausdrückliche Zustimmung der KundenIn oder aufgrund unwirksamer Einwilligungen persönliche Informationen, haben die Verbände noch keine zuverlässige Handhabe. Mit dem neuen Gesetz sind künftig unerwünschte Werbung, das Erstellen von Persönlichkeitsprofilen, Scoring zur Bonitätsprüfung durch Auskunfteien oder Maßnahmen im Adress- und Datenhandel gerichtlich besser angreifbar.

Den Regierungsentwurf vom Februar 2015 hatte das Parlament noch geändert und eingeschränkt. Die Bestimmungen sollen nicht anwendbar sein, wenn personenbezogene Daten einer VerbraucherIn ausschließlich zur Geschäftsabwicklung erhoben, verarbeitet oder genutzt werden. Verbraucherschutzverbände müssen künftig ihre Abmahnpraxis beim Bundesamt für Justiz anzeigen. Damit soll eine Abzocke mit Anwaltsschreiben verhindert werden: Bei Anzeichen von Missbrauch soll die Behörde einschreiten können. Die ParlamentarierInnen unterstreichen, dass insbesondere bei Verstößen kleinerer Unternehmen zunächst „kostenlose schriftliche Hinweise“ versandt werden könnten.

SprecherInnen der Union und der SPD lobten das Gesetz in der abschließenden Lesung als wichtigen Verbraucherschutz. VertreterInnen der Opposition geht der Entwurf nicht weit genug. Der Bundesverband Deutsche Startups, so Verbandschef Florian Nöll, erwartet eine Klagewelle: „Das Verbandsklagerecht schafft eine enorme Zahl von privaten Kontrollinstanzen, die das Potential haben, unsere Startups mit einer Klagewelle zu ertränken.“ Der Gesetzgeber schaffe damit ein „enormes Bürokratiemonster“ (Krempl, Bundestag beschließt Verbandsklagerecht bei Datenmissbrauch, www.heise.de 17.12.2015).

Bund

Regierungsfraktionen für mehr Videoüberwachung nach Silvesterübergriffen

Kurz nach den Silvester-Attacken zum Jahreswechsel 2015/2016 vor allem von nordafrikanischen Männern und vor allem in Köln gegenüber Frauen forderten die Regierungsfraktionen CDU und SPD mehr Polizei und Video-Überwachung. Vor Beginn der CDU-Vorstandsklausur in Mainz hat sich Bundeskanzlerin Angela Merkel dafür ausgesprochen, straffällige Ausländer früher als bislang auszuweisen. Bislang gilt eine Freiheitsstrafe von zwei bis drei Jahren als Richtschnur für eine Ausweisung. „Man verwirkt es früher“, sagte Merkel über das Gastrecht in Deutschland und erhielt dafür lang anhaltenden Applaus der Basis.

CDU und SPD wollen als Konsequenz aus den Übergriffen in mehreren Großstädten außerdem die Überwachung von öffentlichen Plätzen ausweiten. In einer „Mainzer Erklärung“ der CDU heißt es, an „Kriminalitätsbrenn- und Gefahrenpunkten“ sollten mehr Kameras installiert werden. Ähnlich äußerte sich SPD-Fraktionschef Thomas Oppermann nach einer Klausurtagung seiner Abgeordneten in Berlin. Juristische Bedenken wies Oppermann zurück. Er sei der Überzeugung, dass bei Aufzeichnungen an öffentlichen Plätzen das individuelle Persönlichkeitsrecht „hinter das öffentliche Interesse zurücktreten muss; das hat mit einer Überwachungsgesellschaft nichts zu tun“. Da solche Aufnahmen in der Regel nach 24 Stunden gelöscht würden, handele es sich nicht um einen dauerhaften Eingriff in die Rechte einzelner Personen.

Bei anderen möglichen Konsequenzen aus den Vorfällen zum Jahreswechsel liegen die Koalitionspartner noch auseinander. Die SPD-Fraktion dringt vor allem auf mehr PolizistInnen. So sollen bis 2019 insgesamt 12.000 neue Stellen geschaffen werden, je die Hälfte im Bund und in den Ländern. Was Gesetzesänderungen anging, sagte Oppermann: „Ich sehe im Augenblick keinen gesetzgeberischen Handlungsbedarf.“ SPD-Chef Sigmar Gabriel zeigte sich dafür am Rande seiner Kuba-Reise offener: „Wenn es nötig ist, Gesetze zu ändern, werden wir auch das tun“ (Becker/Bauchmüller/Fried, „Gastrecht verwirkt“, www.sueddeutsche.de 08.01.2016 = Koalition will Video-Überwachung ausweiten, SZ 09./10.01.2016, 6).

Bund

SPD will Verfassungsschutz beobachten lassen

Die SPD hat sich für eine Beobachtung der AfD durch die Ämter für Verfassungsschutz ausgesprochen. Nach-

dem die AfD-Chefin Frauke Petry sich für Schusswaffengebrauch gegen Flüchtlinge an den Grenzen eingesetzt hatte, bekräftigte Vizekanzler Sigmar Gabriel die Forderung, die rechtspopulistische Partei durch die Ämter für Verfassungsschutz beobachten zu lassen. Außerdem forderte der SPD-Chef, dass die AfD von TV-Runden im öffentlich-rechtlichen Fernsehen ausgeschlossen werden müsse: „Für mich gehört die AfD in den Verfassungsschutzbericht und nicht ins Fernsehen. Unglaublich, dass solche Parteien ihre Parolen jetzt in öffentlich-rechtlichen Rundfunksendern absondern dürfen. Früher galt in Deutschland eine klare Regel: Parteien, die sich gegen die freiheitlich-demokratische Grundordnung unseres Landes wenden, denen helfen wir nicht noch, ihre Propaganda über das Fernsehen zu verbreiten."

Gabriel sieht die Partei im Konflikt mit dem Grundgesetz: „Bei der AfD gibt es massive Zweifel, dass sie auf der freiheitlich-demokratischen Grundordnung der Republik steht. Da geht es nicht nur um schräge Forderungen wie die Petrys, dass alle Frauen mindestens drei Kinder bekommen sollten. Sondern die Dame will an der deutschen Grenze auf unbewaffnete Flüchtlinge schießen lassen." Petry sei in Dresden geboren und müsse eigentlich wissen, was es heiße, wenn an einer Grenze auf Menschen geschossen wird. Am 08.01.2016 hatte schon die SPD-Bundestagsfraktion beschlossen, die AfD müsse wegen ihrer gefährlichen rechtsextremen Tendenzen beobachtet werden. Die AfD reagierte mit einer Einladung: „"Lieber Herr Gabriel, bitte verstecken Sie sich nicht hinter dem Verfassungsschutz!" Man lade ihn zu den AfD-Sitzungen ein (AfD laut Gabriel ein Fall für den Verfassungsschutz, www.zeit.de 31.01.2016; SPD: AfD überwachen, SZ 09./10.01.2016, 8).

Baden-Württemberg

Polizei erhält Bodycams

Wie zuvor andere Bundesländer macht nun das grün-rot regierte Baden-Württemberg den Weg frei für den Test von „Bodycams", also am Körper von PolizistInnen getragenen Videokameras. Der Einsatz dieser Körperkameras soll Gewalt gegen PolizistInnen verhindern und abschreckend wirken. Die Maßnahme gehört zu einem Paket, mit dem Innenminister Reinhold Gall (SPD) auf die Silvester-Vorfälle in Köln reagiert. Die BeamtIn, welche die Kamera auf der Schulter trägt, hat auf ihrer Weste die Aufschrift „Videoaufzeichnung". Die Kamera wird mit Knopfdruck aktiviert, so der Bundesvorsitzende der Gewerkschaft der Polizei (GdP) Oliver Malchow, „wenn Worte nicht mehr ausreichen". Er sei lange skeptisch gewesen, weil die Aufzeichnung ein Eingriff in Bürgerrechte ist. Aber ein Pilotversuch in Frankfurt habe ihn überzeugt, wo Übergriffe auf PolizistInnen signifikant abgenommen hätten.

Die GDP plädiert für eine deutschlandweite Einführung von Bodycams, da überall im Land die Zahl der Übergriffe steige. Malchow bezweifelt jedoch, dass die Körperkamera dafür geeignet gewesen wäre, auf dem Kölner Domplatz Beweise zu sichern. Doch sei die innere Sicherheit in den letzten Jahren sträflich vernachlässigt worden; die Sexualdelikte in der Silvesternacht hätte nun eine „Initialzündung" abgegeben. 2011 hatte die neue grün-rote Landesregierung in Stuttgart eine nichtnamentliche Kennzeichnungspflicht mit Nummern von PolizeibeamtInnen einführen wollen. Hintergrund waren die maßlosen Polizeiübergriffe gegen GegnerInnen des Bahnprojektes Stuttgart 21, die das Vertrauen in die Polizei erschüttert hatten. Danach hatte die SPD, die bedacht ist auf ihr Markenzeichen der inneren Sicherheit, diese Maßnahme fünf Jahre lang verschleppt. Es wurde zum Running Gag, dass die Kretschmann-Regierung es zwar nicht zulässt, dass die BürgerInnen die Polizei identifiziert, wohl aber umgekehrt. Ministerpräsident Winfried Kretschmann begründete den Bodycam-Vorstoß damit, dass das Sicherheitsgefühl der Menschen seit der Silvesternacht „beeinträchtigt" sei. In Stuttgart, Mannheim und Freiburg soll getestet werden. Die Fraktion der Grünen, die lange Zeit datenschutzrechtliche Bedenken hegte, hat in der Vorwahlzeit Zustimmung signalisiert. Am 13.03.2016 sind Landtagswahlen (Kelnberger, Vorsicht Kamera, SZ 03.02.2016, 1).

Bayern

Verfassungsschutz darf an TK-Verkehrsvorratsdaten ran

Die Bayerische Landesregierung hat am 15.12.2015 den Entwurf eines Landesgesetzes beschlossen, wonach das dortige Landesamt für Verfassungsschutz (LfV) künftig auf Daten aus der Vorratsspeicherung von Telekommunikations- (TK-) Verkehrsdaten zugreifen darf. Das im Oktober 2015 vom Bundestag und am 06.11.2015 vom Bundesrat beschlossene Gesetz verpflichtet Telekommunikationsanbieter, die Festnetz- und Mobilverbindungen ihrer KundInnen für zehn Wochen aufzubewahren. Gespeichert wird, wer mit wem, wann, wie lange, von wo aus und mit welchem Gerät kommuniziert hat. In erster Linie sollen die Daten Polizei und Staatsanwaltschaft bei der Strafverfolgung helfen. Bundesinnenminister Thomas de Maizière (CDU) meinte: „Mit dem ausgewogenen Gesetz geben wir unserer Polizei ein wichtiges Instrument für die Verbrechensbekämpfung".

Eine Klausel im Gesetz ermöglicht es den Ländern, die Daten auch zur Gefahrenabwehr zu nutzen. Innenminister Joachim Herrmann (CSU) kommentierte: „Es kann nicht sein, dass unsere Nachrichtendienste weniger wissen als Polizei und Strafverfolgungsbehörden". Er sei überzeugt, dass das Gesetz zur Vorratsdatenspeicherung „diese Möglichkeit jetzt auch für den Verfassungsschutz eröffnet". Ex-Bundesjustizministerin Sabine Leutheusser-Schnarrenberger (FDP) kritisierte die Offenheit der rechtlichen Bundesregelung: „Jetzt rächt sich die Neuauflage der Vorratsdatenspeicherung". Das Gesetz enthalte „unklare Regelungen, die einer totalen Überwachung Tür und Tor öffnen". Herrmann dagegen meinte, der Verfassungsschutz gehöre auch zu den Gefahrenabwehrbehörden. Der bayerische Vorstoß sei keine Durchbrechung des Prinzips der Trennung von Verfassungsschutz und Polizei, sondern gerade dessen Bestätigung, wenn man für den Verfassungsschutz eine eigene Ermächtigungsgrundlage für den Zugriff auf die Daten schaffe. Er zeigte sich überzeugt, dass Bund und Länder Bayern bald

folgen werden. Er hatte die Kabinettssitzung geleitet, da Ministerpräsident Horst Seehofer abwesend war.

Im Bundesjustizministerium sieht man das ganz anders. Justizminister Heiko Maas (SPD) hatte während der Gesetzgebungsprozedur erklärt: „Der Verfassungsschutz ist in dem Gesetz nicht vorgesehen für einen Zugriff nach den Regeln, die wir in diesem Gesetz vorschlagen." Einen ausdrücklichen Ausschluss enthält das Gesetz aber auch nicht. Über die Verwendung der Daten heißt es in dem neuen § 113c des Telekommunikationsgesetzes (TKG), dass die gespeicherten Daten „an eine Gefahrenabwehrbehörde der Länder übermittelt werden, wenn diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr die eigene Erhebung der Daten zur Abwehr einer konkreten Gefahr für Leib Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes erlaubt, verlangt". In der Gesetzesbegründung ist nur die Polizei erwähnt, nicht der Verfassungsschutz (Verfassungsschutz greift auf Verbindungsdaten zu, SZ 16.12.2015, 29; Prantl, „Wie eine ewige Krankheit", SZ 18.12.2015, 5).

Berlin

Maja Smoltczyk folgt Alexander Dix als Datenschutzbeauftragte

Die Juristin Maja Smoltczyk ist Berlins neue Datenschutzbeauftragte. Die 54 Jahre alte bisherige Abteilungsleiterin im Abgeordnetenhaus wurde am 28.01.2016 in namentlicher Abstimmung gewählt. Smoltczyk erhielt 75 Ja- und 60 Nein-Stimmen, 9 Abgeordnete enthielten sich. Die Opposition hatte zuvor noch einen Antrag gestellt, den Wahlgang zu verschieben. Das lehnten SPD und CDU ab. Smoltzcyk folgt Alexander Dix nach. Dessen langjährige Amtszeit war bereits am 2. Juni 2015 zu Ende gegangen.

Die Fraktionsvorstände von SPD und CDU hatten sich nach monatelanger Suche am 12.01.2016 auf diese Personalie geeinigt. Smoltczyk war zuvor Leiterin der Abteilung Plenum und Ältestenrat sowie des Kulturellen Kuratoriums Louise-Schroeder-Medaille im Abgeordnetenhaus, für das sie seit 1994 tätig war. Ihre Aufgabe war die Betreuung der Ausschüsse und die Sorge, dass Abläufe korrekt eingehalten würden und Papiere vollständig vorliegen. Nebenberuflich arbeitet Smoltczyk als Bildhauerin. Für das Abgeordnetenhaus (AGH) schuf sie eine Büste des früheren Präsidenten Walter Momper (SPD).

Ein besondere Nähe Smoltczyks zu digitalen Themen ist bislang nicht bekannt. Der frühere Piratenpolitiker und Berliner Abgeordnete Christopher Lauer twitterte nach ihrer Nominierung: „Fängt gut an, die Datenschutzbeauftragte in spe hat keine Datenschutzerklärung auf ihrer Webseite http://www.bildhauerin-berlin.de". Sein früherer Ex-Kollege Martin Delius ergänzte per Twitter: „Ich halte Maja Smoltczyk für eine sehr gute Mitarbeiterin der AGH-Verwaltung. Als Datenschutzbeauftragte kann ich sie mir nicht vorstellen."

Berlins langjähriger Datenschutzbeauftragter Dix war auf Bitten des Präsidiums des Abgeordnetenhauses bis zur Regelung seiner Nachfolge im Amt geblieben. Er hatte auf einen Kommunikationsprofi als Nachfolger gehofft. „Ich würde mir wünschen, dass er die Diskussion über das Internet der Dinge und Big Data und die entsprechenden Antworten des Datenschutzes noch viel stärker in die Gesellschaft trägt. Man muss darüber nachdenken, wie man das Nicht-Fassbare gegenständlich und sinnlich erfahrbar macht. Da könnten nicht-juristische Formen der Thematisierung wie Kunst, Comics und andere Formen der Kommunikation wie Computerspiele und Apps eine wichtige Rolle spielen".

Als die Absicht der Regierungsfraktionen bekannt wurde, wandte sich der Vorstand der Deutschen Vereinigung für Datenschutz e. V. (DVD) mit einem offenen Brief an die Fraktionen des Abgeordnetenhauses, der hier dokumentiert werden soll:

„Sehr geehrte XX,

die Deutsche Vereinigung für Datenschutz e. V. (DVD) hat zur Kenntnis genommen, dass die Regierungsparteien im Berliner Abgeordnetenhaus planen, am 28.01.2016 als Nachfolgerin von Alexander Dix in das Amt der Berliner Beauftragten für Datenschutz und Informationsfreiheit Frau Maja Smoltczyk zu wählen. Dieses Vorhaben ist beim Vorstand der DVD auf seiner Sitzung am 16.01.2016 in Berlin auf Irritation und Besorgnis gestoßen. Dass Kompetenzen im Bereich des Datenschutzes und der Informationsfreiheit für die Auswahl der Kandidatin eine Rolle spielten, ist für die DVD nicht erkennbar. Dies stößt auf erhebliche Kritik. Art. 33 Abs. 2 GG fordert, dass öffentliche Ämter nach Eignung, Befähigung und fachlicher Leistung zu besetzen sind.

Es ist verfassungs- und europarechtliche Aufgabe der Datenschutzbeauftragten, auf der Grundlage besonderer technischer und rechtlicher Qualifikation und einer unabhängigen Stellung institutionell digitalen Grundrechtsschutz zu gewährleisten. Die Bestellung von Datenschutzbeauftragten setzt entsprechende Kenntnisse voraus. Nur so können Datenschutzbeauftragte in Augenhöhe mit Behörden und Unternehmen kommunizieren und sich mit diesen auseinandersetzen. Deswegen muss sich die zu bestellende Person im Bereich des Datenschutzes und der Informationsfreiheit schon betätigt haben. Nur so ist auch erkennbar, dass und wie diese den sich stellenden künftigen Anforderungen gerecht werden kann.

Soweit für uns erkennbar, liegen diese Voraussetzungen bei der Berliner Kandidatin nicht vor. Damit würde sich eine Praxis fortsetzen, die sich nicht nur auf Länder-, sondern auch auf Bundesebene zu etablieren scheint. Bei der Bestellung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Dezember 2013 wurde kein Wert auf Fachkompetenz gelegt. Sichtbares Ergebnis ist auf Bundesebene, dass die Amtsinhaberin ihre Aufgaben nicht wirkungsvoll erfüllt. Dies hat Wirkung für die Wahrnehmung der Kontroll- und Beratungstätigkeit der Bundesbeauftragten. Darüber hinausgehend leidet darunter auch das Ansehen des deutschen Datenschutzes in Europa und in der Welt.

Der bisherige Berliner Datenschutzbeauftragte Alexander Dix konnte schon bei seiner Bestellung internationales Renommee als Fachmann in Fragen des Datenschutzes und der Informationsfreiheit vorweisen. Der Erfolg seiner Tätigkeit in Berlin, bundesweit wie auch international bestätigte die

Richtigkeit dieser Wahl. Alexander Dix repräsentierte das Anliegen des digitalen Grundrechtsschutzes wie auch den institutionellen Datenschutz auf europäischer und internationaler Ebene in hervorragender Weise. Die DVD dankt ihm hierfür. Es ist nicht absehbar, dass die Lücke, die durch den Weggang von Alexander Dix entsteht, mit den jetzigen Planungen gefüllt werden kann.

Der Vorstand der DVD fordert deshalb die Koalitionsfraktionen im Berliner Abgeordnetenhaus auf, ihre Personalauswahl zu überdenken. Dabei sollte neben fachlicher Kompetenz auch das Ziel verfolgt werden, eine größtmögliche Zustimmung im Abgeordnetenhaus bei der Bestellung zu erreichen.

Mit freundlichen Grüßen gez. Frank Spaeing Vorsitzender der Deutschen Vereinigung für Datenschutz e. V.“

Die Berliner Datenschutzbehörde gehörte bisher zu den Perlen der deutschen Datenschutzaufsicht. Ausgestattet mit 39 Vollzeitstellen ist sie – gemessen an der Bevölkerungszahl in den Bundesländern – eine der größten Datenschutzaufsichtsbehörden Deutschlands.

Grüne, Linke und Piraten bezweifelten nach deren Wahl die fachliche Kompetenz von Smoltczyk. Die Gewählte verfüge über keine einschlägigen Erfahrungen in Sachen Datenschutz und Informationsfreiheit (Maja Smoltczyk ist Berlins neue Datenschutzbeauftragte, www.berlin.de 28.01.2016; Offener Brief der DVD zur Nominierung der Kandidatin für die Berliner Beauftragte für Datenschutz und Informationsfreiheit vom 16.01.2016, www.datenschutzverein.de 18.01.2016; Juristin und Bildhauerin folgt auf Alexander Dix, www.golem.de 12.01.2016).

Schleswig-Holstein

ULD kritisiert polizeiliche Funkzellenabfragen

Die stellvertretende schleswig-holsteinische Datenschutzbeauftragte und Vize-Chefin des Unabhängigen Landeszentrums für Datenschutz (ULD) Barbara Körffer kritisierte am 11.11.2015 gegenüber dem Rechtsausschuss des Kieler Landtags die Praxis der Funkzellenabfragen durch Polizei und Staatsanwaltschaften und forderte Korrekturen. Es werde vor allem nicht hinreichend dargelegt, inwiefern die Abfragen überhaupt nötig und verhältnismäßig seien, sie mahnte mehr Transparenz an.

Sie stellte einen Prüfbericht des ULD zu Funkzellenabfragen aus den Jahren 2009 bis 2012 vor, in dem eine Stichprobe von zehn Funkzellenabfragen unter die Lupe genommen wurde. Bei der umfangreichsten davon sind allein rund 7000 Datensätze auf einen Schlag erhoben worden. Funkzellenabfragen erzeugen dem ULD zufolge generell „in besonderem Maße eine Gefahr für Unbeteiligte, in die Ermittlungen einbezogen zu werden“. Körffer führte aus, dass die Polizei damit Informationen bekomme über den Ort eines Telefongesprächs, verschickte und eingehende SMS sowie Internetverbindungen. Dies allein bringe aber noch keinen großen Erkenntnisgewinn, sodass in der Regel Abgleiche mit ähnlichen Abfragen von anderen Tatorten oder weiteren Daten etwa über das Polizeisystem Artus durchgeführt würden.

Die rechtlichen Voraussetzungen für derartige Handy-Rasterungen sind laut Körffer recht hoch gehängt. Es müsse eine Straftat von „erheblicher Bedeutung“ vorliegen, was bei den geprüften Fällen zugetroffen habe. Das Instrument dürfe aber erst genutzt werden, wenn Ermittlungen auf andere Weise wenig aussichtsreich seien. Diese Voraussetzung sei nicht immer erfüllt gewesen. Teils hätten die Fahnder keine Idee gehabt, was sie mit dem Ergebnis anstellen sollten. Es seien „vorsorglich Funkzellendaten gesichert“ worden. Die Daten müssten speziell gekennzeichnet werden, was „nicht immer erkennbar war“. Betroffene seien zudem in den meisten Fällen nicht benachrichtigt worden, nachdem ihre Bestandsdaten ermittelt worden seien. Die erhobenen Informationen seien anschließend teils auch gar nicht gelöscht worden.

Körffer plädierte dafür, die Daten zu entsorgen, wenn diese „gegenwärtig“ nicht mehr gebraucht würden. Zudem sollte der Gesetzgeber ein „Quick Freeze“ einführen: Bei dem Verfahren werden die begehrten Informationen beim Provider eingefroren und zu einem späteren Zeitpunkt abgefragt werden, wenn dies erforderlich sei. Auch die vom Bundestag kurz zuvor beschlossene vierwöchige Vorratsspeicherung von Standortdaten helfe in dieser Hinsicht nicht viel und sei kein Ersatz für ein solches gezieltes Vorgehen.

Der Landtag hatte die Analyse in Auftrag gegeben, nachdem eine Anfrage der Piratenfraktion 2013 ergeben hatte, dass nicht einmal jede 20. Funkzellenabfrage zu einer Verurteilung geführt hat. Parallel werden immer mehr Handynutzern in Schleswig-Holstein mithilfe des Instruments überwacht: Während 2012 noch 256 Funkzellenabfragen erfolgten, waren es 2013 schon 441. 2014 schnellte die Zahl auf 569 weiter hoch.

Ein Vertreter des Landesinnenministeriums erklärte: „Wir sind in der Polizei unzufrieden mit dem Prüfbericht.“ Alle Abfragen seien gerichtlich angeordnet worden. Zudem habe das ULD eine Handlungsweisung aus dem ersten Halbjahr 2014 nicht berücksichtigt, mit der Schwachstellen abgestellt worden seien. Körffer erwiderte, dass dieser Erlass nur die Datenverarbeitung der Polizei betreffe und den Hinweis auf die Kennzeichnungspflicht aufgegriffen habe. Die anderen Punkte würden nicht erfasst. Es sei allgemein schwierig, den Erfolg von Funkzellenabfragen zu messen, da diese in der Regel in einem Bündel mit anderen Instrumenten eingesetzt würden (Krempl, Schleswig-Holstein: Datenschützerin rügt Handy-Rasterfahndung, www.heise.de 11.11.2015; ULD, http://www.landtag.ltsh.de/infothek/wahl18/umdrucke/5000/umdruck-18-5038.pdf).

Datenschutznachrichten aus dem Ausland

Europa

Einigung über Datenschutz-Paket im Trilog

Vertreter des Europaparlaments, des Rates der Europäischen Union (EU) und der EU-Kommission haben sich im sog. Trilog am 15.12.2015 nach jahrelangem Ringen im Rahmen einer Datenschutzreform auf den Text einer Europäischen Datenschutz-Grundverordnung (EU-DSGVO) geeinigt, welche die europäische Datenschutz-Richtlinie aus dem Jahr 1995 ablösen soll. Einigung wurde zudem gefunden über eine Europäische Datenschutzrichtlinie für Polizei und Justiz.

Im Vorfeld dieser Einigung gab es hitzige Diskussionen. Gestritten wurde u. a. über Mindestalter bei sozialen Netzwerke. Kinder und Jugendliche dürfen in einigen europäischen Ländern Online-Dienste wie Facebook oder WhatsApp künftig bis zu einem Alter von 16 Jahren nur mit Zustimmung ihrer Eltern nutzen. In anderen Ländern wird die Altersgrenze bei 13 liegen. Lobbyisten von US-Technologiefirmen waren, so Presseberichte, noch in letzter Minute erneut in die Offensive gegangen, um geringere Schutzstandards zu erreichen.

Die Datenschutzbehörden werden künftig in einem sog. Kohärenzverfahren enger zusammenarbeiten, um grenzüberschreitende Fälle unter anderem mithilfe einer zentralen Kontaktstelle zu lösen. Die bisherige Artikel-29-Arbeitsgruppe wird zum Europäischen Datenschutzausschuss mit eigener Rechtspersönlichkeit und der Möglichkeit, Mehrheitsentscheidungen zu treffen. Gegen Unternehmen können Strafen von bis zu vier Prozent der Jahresumsätze verhängt werden, wenn sie gegen die Datenschutzregeln verstoßen.

Betroffenenrechte

Die neuen Vorschriften sollen die bestehenden Rechte der BürgernInnen stärken und diesen mehr Kontrolle über ihre Daten geben. Im Mittelpunkt stehen folgende Aspekte:

- Einfacherer Zugang zu den eigenen Daten: Es wird besser über die Art und Weise, wie die Daten verarbeitet werden, informiert. Diese Informationen müssen klar und verständlich sein.
- Recht auf Datenübertragbarkeit: Personenbezogene Daten können einfacher von einem Anbieter auf einen anderen übertragen werden.
- „Rechts auf Vergessenwerden“: Wenn die Betroffenen nicht möchten, dass ihre Daten weiter verarbeitet werden, und es keine legitimen Gründe für deren Speicherung gibt, müssen die Daten gelöscht werden.
- Breach Notification: Unternehmen und Organisationen müssen insbes. die nationale Aufsichtsbehörde so bald wie möglich über schwere Verstöße gegen den Datenschutz informieren, damit die Nutzer geeignete Maßnahmen ergreifen können.

Hat eine VerbraucherIn ein Problem mit einem Anbieter in einem anderen EU-Land, soll sie sich künftig in ihrer Sprache an die heimische Beschwerdestelle wenden können.

Vorschriften für Unternehmen

Wegen der enormen wirtschaftlichen Bedeutung von personenbezogenen Daten für die heutige digitalisierte Wirtschaft, etwa im Bereich der Massendaten (Big Data), sollen durch die Vereinheitlichung der europäischen Datenschutznormen neue Geschäftsmöglichkeiten und Chancen für Innovation geschaffen werden.

- Harmonisierung der Regelungen: Durch die Verordnung wird ein einheitliches Regelwerk geschaffen, das Unternehmen die Geschäftstätigkeit in der EU erleichtern und Kosten sparen soll. Datenschutz-Oasen soll es in Europa nicht mehr geben.
- One-Stop-Shop: Unternehmen haben zumeist nur noch mit einer einzigen Aufsichtsbehörde zu tun. Damit sollen pro Jahr ca. 2,3 Mrd. € eingespart werden.
- Marktortprinzip: Unternehmen mit Sitz außerhalb Europas müssen dieselben Regeln befolgen, wenn sie Dienstleistungen in der EU anbieten.
- Risikobasierter Ansatz: Mit den neuen Regeln wird statt einer aufwändigen allgemeinen Verpflichtung eine den jeweiligen Risiken angepasste Verpflichtung zu Datenschutzvorkehrungen eingeführt.
- Technischer Datenschutz: Die Verordnung soll gewährleisten, dass die Datenschutzgarantien von der frühesten Entwicklungsphase an in die Produkte und Dienstleistungen eingebaut werden („Datenschutz durch Technik“). Datenschutzfreundliche Techniken wie Pseudonymisierung werden gefördert, um die Vorteile von massendatenbezogenen Innovationen bei gleichzeitigem Schutz der Privatsphäre nutzen zu können.
- Entlastung für kleinere Unternehmen: Von der Datenschutzreform sollen durch geringere Kosten und weniger Verwaltungsaufwand, insbesondere für kleine und mittlere Unternehmen (KMU), Impulse für das Wirtschaftswachstum ausgehen. Die EU-Datenschutzreform soll KMU dabei helfen, in neue Märkte vorzudringen. Nach den neuen Vorschriften wird sich der Verwaltungsaufwand für KMU in vier Punkten reduzieren: 1. Aufhebung der Meldepflicht: Mitteilungen an die Aufsichtsbehörden sind eine Formalität, die bei den Unternehmen jedes Jahr angeblich mit 130 Mio. € zu Buche schlägt. Die Meldepflicht wird durch die Reform vollständig beseitigt. 2. Gebühren: Wenn Anträge auf Zugang zu den Daten offensichtlich unbegründet oder unverhältnismäßig sind, können KMU in Zukunft Gebühren für die Bereitstellung des Zugangs verlangen. 3. Datenschutzbeauftragte: KMU sind nicht verpflichtet, einen Datenschutzbeauftragten zu ernennen, es sei denn, die Datenverarbeitung ist ihr Kerngeschäft. 4. Folgenabschätzung: KMU sind nicht verpflichtet, eine Folgenabschätzung durchzuführen, es sei denn, es besteht ein hohes Risiko.

Datenschutzrichtlinie für Polizei und Justiz

Mit einer neuen Datenschutzrichtlinie für Polizei und Strafjustiz sollen die Strafverfolgungsbehörden in den Mitgliedstaaten ermittlungsrelevante Informationen effizienter und wirksamer austauschen und besser bei der Bekämpfung von Terrorismus und sonstiger schwerer Kriminalität in Europa zusammenarbeiten können (dazu ausführlich obiger Beitrag auf S. 8). Sie hat den Anspruch, die unterschiedlichen Rechtstraditionen der Mitgliedstaaten zu respektieren und soll voll und ganz im Einklang mit der Charta der Grundrechte stehen.

Personenbezogene Daten sollen besser geschützt werden, wenn sie für Zwecke der Strafverfolgung verarbeitet werden, wozu auch die Kriminalitätsprävention gehört. Der Schutz gilt für jedermann – unabhängig davon, ob es sich um ein Opfer, einen Straftäter oder Zeugen handelt. Die Datenverarbeitung in den Polizeibehörden und Staatsanwaltschaften der Union muss den Grundsätzen der Notwendigkeit, Verhältnismäßigkeit und Rechtmäßigkeit genügen und mit angemessenen Vorkehrungen zum Schutz des Individuums einhergehen. Sie unterliegt der Aufsicht durch unabhängige nationale Datenschutzbehörden, und es muss für einen wirksamen Rechtsschutz gesorgt werden. Die Richtlinie für den Datenschutz bei Polizei und Strafjustiz enthält Regeln für den Transfer personenbezogener Daten aus der EU, um zu gewährleisten, dass der in der EU dem Einzelnen garantierte Datenschutz nicht ausgehöhlt wird.

Kommentare

Andrus Ansip, Vizepräsident für den digitalen Binnenmarkt, kommentierte die Einigung: „Mit der heutigen Einigung sind wir dem digitalen Binnenmarkt ein gutes Stück näher gekommen. Dank solider gemeinsamer Standards für den Datenschutz können unsere Bürgerinnen und Bürger sicher sein, dass sie die Kontrolle über ihre personenbezogenen Daten behalten. Und sie können alle Dienstleistungen und Chancen eines digitalen Binnenmarkts nutzen. Wir sollten den Schutz der Privatsphäre und den Datenschutz nicht als Hemmschuh für wirtschaftliches Handeln begreifen. Im Gegenteil: Sie sind ein wesentlicher Wettbewerbsvorteil. Als nächstes gilt es, ungerechtfertigte Hemmnisse zu beseitigen, die den grenzüberschreitenden Datenfluss beschränken, wie örtliche Gepflogenheiten und bisweilen nationales Recht, die die Speicherung und die Verarbeitung bestimmter Daten außerhalb des nationalen Hoheitsgebiets begrenzen.

Die EU-Kommissarin für Justiz, Verbraucher und Gleichstellung, Věra Jourová ergänzte: „Heute haben wir das Versprechen der Juncker-Kommission eingelöst, dass wir die Datenschutzreform 2015 abschließen werden. Harmonisierte Datenschutzvorschriften für die Polizei- und Strafverfolgungsbehörden werden die Zusammenarbeit der Mitgliedstaaten bei der Strafverfolgung auf der Grundlage gegenseitigen Vertrauens erleichtern und so einen Beitrag zur europäischen Sicherheitsagenda leisten."

Der EU-Parlamentarier Axel Voss von der CDU warnte vor negativen Folgen für die Wirtschaft: „Wir müssen aufpassen, dass dies am Ende nicht ein Hemmschuh für die europäische Industrie und Forschung wird."

Nächste Schritte

Im Anschluss an die im Trilog erzielte politische Einigung sollen die Texte in ihrer endgültigen Fassung Anfang 2016 vom Europäischen Parlament und vom EU-Rat förmlich angenommen werden. Zwei Jahre danach ist das Inkrafttreten der neuen Vorschriften vorgesehen.

Die Kommission will eng mit den Datenschutzbehörden der Mitgliedstaaten zusammenarbeiten, um eine einheitliche Anwendung der neuen Vorschriften zu gewährleisten. Während der zweijährigen Übergangsphase wird die Kommission die Bürgerinnen und Bürger über ihre Rechte und die Unternehmen über ihre Pflichten informieren (EU-Kommission, Einigung über die EU-Datenschutzreform der Kommission wird digitalen Binnenmarkt voranbringen, PE 15.12.2015; Neue EU-Datenschutzregeln: Facebook erst ab 16 Jahren, www.heise.de 16.12.2015).

Europa

Europol fordert Datenaustausch über Internet-Überwachung

Die europäische Polizeibehörde (Europol) verlangt für sein neues „Hinweiszentrum" zur Internetüberwachung neue Befugnisse, um bei Betreibern sozialer Netzwerke Auskunft z. B. über verschiedene mit einer IP-Adresse verknüpfte Konten zu erhalten. Das Zentrum hat im Sommer 2015 seine Arbeit aufgenommen. Es müsse nicht nur selbst erhobene persönliche Daten an private Parteien weiterleiten dürfen, sondern auch von diesen Informationen bekommen können, heißt es in einem Papier der luxemburgischen EU-Ratspräsidentschaft von Ende September 2015. Um insbesondere terroristische Bedrohungen ausmachen zu können, sei ein „Dialog" unverzichtbar.

Im Kern geht es der europäischen Polizeibehörde um einen Auskunftsanspruch für Bestands- und Nutzungsdaten vor allem bei Betreibern sozialer Netzwerke. Facebook etwa müsse bei einen Hinweis von Europol verpflichtet sein, die FahnderInnen über weitere Konten und Profile aufzuklären, die eine mit einer bestimmten IP-Adresse verknüpfte Person habe.

Für andere Diensteanbieter sollten demnach gleiche Anforderungen gelten, da diese generell einen „guten Überblick über die Aktivitäten ihrer Kunden auf ihrer eigenen Plattform" hätten. Aber auch Daten, die Internetfirmen unter anderem mithilfe von Cookies und anderen Trackingverfahren über die Surfgewohnheiten ihrer Nutzenden auf anderen Portalen sammeln, stehen auf der Wunschliste der Strafverfolger. Ein Praxisbeispiel im Schreiben dreht sich um Facebook: Nach Ansicht der Polizeibehörde müsse das Netzwerk in der Position sein, auf eine Europol-Anfrage reagieren zu können, wenn das Netzwerk wisse, dass von der gleichen IP-Adresse aus oder von der gleichen Person weitere Accounts betrieben werden, die Europol bislang nicht entdeckt hat. Weiter heißt es: „Dasselbe gilt für andere Dienstanbieter, die allgemein einen sehr guten Überblick über die Nut-

zeraktivität auf ihrer eigenen Plattform haben."

Die Ratsspitze hat sich bereits hinter Europols Wunsch gestellt und einen Änderungsantrag für die laufende Reform der Europol-Verordnung in die Verhandlungen mit dem EU-Parlament und der EU-Kommission eingebracht, obwohl den europäischen Fahndern eigentlich keine „operativen Befugnisse" zustehen. Der angemahnte „Datenaustausch" dürfte demnach in „spezifischen Fällen" erfolgen, solange dem nicht die Grundrechte der Betroffenen entgegenstünden. Verhandlungsführer der Abgeordneten sehen den Antrag zwar noch skeptisch, doch viele Mitgliedsstaaten dürften hinter dem Luxemburger Vorschlag stehen.

Die Bundesregierung begrüßt die vorgesehene „Kooperation" der „Internet Referal Unit" (IRU) Europols mit den beteiligten EU-Ländern und der Internetwirtschaft grundsätzlich genauso wie den Änderungsvorschlag der Ratspräsidentschaft. Mitgliedsstaaten könnten über eine nationale Kontaktstelle wie das Bundeskriminalamt (BKA) dem Hinweiszentrum themenspezifische Internetinhalte vor allem zu terroristischer Propaganda melden, so eine Antwort des Bundesinnenministeriums auf eine Anfrage der Linksfraktion des Bundestags. Die IRU könne aber auch selbst Online-Kommunikation „identifizieren".

Wenn ein Bezug zu weiteren EU-Ländern ersichtlich ist, solle das Europol-Zentrum deren Kontaktstellen informieren und „um Rückmeldung bitten, ob die Meldung an den betroffenen Internetdiensteanbieter erfolgen kann". Wenn dem nicht widersprochen werde, könnten sich die Den Haager FahnderInnen direkt an den Diensteanbieter wenden. Auch könne Europol personenbezogene Daten aus öffentlich zugänglichen Quellen einschließlich „kommerzieller Informationsanbieter" direkt einholen und verarbeiten.

Die Arbeit der IRU muss sich laut Bundesregierung nicht auf die zunächst vorgesehenen Terrorismushinweise beschränken. Vielmehr könnten auch „Straftaten im Bereich des gewaltbereiten Extremismus in die Zuständigkeit" fallen, was Phänomene wie Hasskommentare, Online-Hetze oder Fremdenfeindlichkeit nicht ausschließe. Dies müsse aber einzeln geprüft werden. Auf die Frage, ob zudem „Schleusungskriminalität" einbezogen werden sollte, antwortete das Innenministerium: Es sei eine Formulierung in der neuen Europol-Verordnung zu finden, die es der Hinweisstelle erlaube, „flexibel auf veränderte Anforderungen zu reagieren".

Europol hatte gemeinsam mit der internationalen Polizeiorganisation Interpol Mitte Oktober 2015 bereits ein Forum durchgeführt, um „Fluchthilfe-Netzwerke" besser bekämpfen zu können. Beteiligt war neben zahlreichen Ländern und Organisationen auch die US-Firma Western Union. Mit Daten des Bargeldtransfer-Anbieters könnten die Strafverfolger etwa ermitteln wollen, an wen Geflüchtete Finanzmittel überwiesen haben. Ein Vertreter von Twitter klärte die Forumsteilnehmenden zudem über die Nutzung des Internets „als Mittel der Kommunikation zwischen Fluchthelfern und Flüchtlingen" auf.

Mit dem Projekt „Check the Web", das hauptsächlich auf das BKA zurückgeht, hat sich Europol bereits seit 2007 ähnlich ausgerichtet wie die IRU. Die Behörde gleiche die mit der neuen Hinweisstelle identifizierten Inhalte mit diesem älteren „Auswerteschwerpunkt" ab, so die Bundesregierung. Geplant sei, bereits bekannte Bezüge festzustellen und beide Einheiten zu verknüpfen.

Laut dem Bundestagsabgeordneten Andrej Hunko von den Linken sollen die beiden Projekte zusammen etwa mit Abteilungen zum Austausch von Finanz- oder Fluggastdaten mit den USA in ein „Europäisches Zentrum zur Terrorismusbekämpfung" bei Europol integriert werden. Jede weitere Kompetenzübertragung zu einer Daten-Superbehörde sei „ein Schritt zur Entdemokratisierung", da die ständig wachsenden Befugnisse kaum mehr kontrolliert werden könnten (Krempl, Internetüberwachung: Europol will an Daten von Facebook und Twitter, www.heise.de 10.11.2015; Europol will mehr Rechte für die Internetüberwachung, www.spiegel.de 09.11.2015).

Europa

EU-Rat fordert neue Initiative zu TK-Vorratsdatenspeicherung

Eine Mehrheit der Delegationen im Rat der Europäischen Union (EU) hat die EU-Kommission aufgefordert, eine neue Initiative zum anlasslosen Protokollieren von Telekommunikations-Nutzungsspuren zu starten. In ihren Ländern halten sie das Instrument weiter für zulässig. Sämtliche EU-Mitgliedsstaaten sehen sich durch das Urteil des Europäischen Gerichtshofs (EuGH) vom 08.04.2014 (C-293/12, C-594/14), mit dem die EU-Richtlinie zur Vorratsspeicherung von Telekommunikations-(TK-) Daten (RL 2006/24/EG) aufgehoben wurde, nicht an einer nationalen Regelung gehindert. Sie waren sich bei einem Ratstreffen der Justiz- und Innenminister am 05.12.2015 in Brüssel einig, dass Verbindungs- und Standortdaten weiter „massenhaft" in „allgemeiner Form" aufbewahrt und Strafverfolgern zugänglich gemacht werden dürften.

Die Mehrheit der nationalen Regierungen hält es demnach auch für nötig, wieder eine EU-weite Grundlage zum anlasslosen Protokollieren von Nutzerspuren zu schaffen, damit dies nicht weiter „fragmenthaft" geschieht. Die Mehrheit der Mitgliedsstaaten appellierte deshalb an die EU-Kommission, ein neues Gesetz auf den Weg zu bringen. Die EU-Staatsanwaltschaft Eurojust und der von der luxemburgischen Präsidentschaft angehörte „Experte" hatten vor der Ratssitzung betont, die Effizienz der Strafverfolgung auf nationaler Ebene werde durch die Fragmentierung beeinflusst. Es gebe etwa Probleme, Telekommunikationsdaten als Beweismittel vor Gericht heranzuziehen sowie bei der grenzüberschreitenden Justizkooperation.

Der EuGH hatte die frühere Richtlinie zur TK-Vorratsdatenspeicherung für nichtig erklärt und angezweifelt, ob eine anlasslose Datensammlung und Massenüberwachung überhaupt mit der Grundrechtecharta vereinbar sei. Die Richter warnten, dass damit „sehr genaue Schlüsse auf das Privatleben" Betroffener gezogen werden könnten. Im März 2015 hatte Martin Selmayr, Kabinetts-Chef von Präsident Jean-Claude Juncker, hervorgehoben, dass die EU-Kommission keinen neuen Gesetzesvorschlag plane. Jeder Mitgliedsstaat sei hier auf sich selbst gestellt. Seitdem hat sich an dieser Front wenig getan. Binnenmarktkommissarin Elżbieta Bieńkowska kritisierte vielmehr den deutschen Entwurf des in-

zwischen verabschiedeten Gesetzes zur TK-Vorratsdatenspeicherung (Krempl, EU-Staaten verlangen neuen Anlauf zur Vorratsdatenspeicherung, www.heise.de 08.12.2015).

Frankreich

Regierung verstetigt Notstands-Sicherheitsgesetz

Die französische Regierung hat am 03.02.2016 einen Gesetzentwurf beschlossen mit dem der seit November 2016 geltende Ausnahmezustand zur Bekämpfung des islamistischen Terrorismus neuerlich verlängert werden soll. Neben schnelleren Festnahmemöglichkeiten sieht der Entwurf Abhörmaßnahmen und Kontrollen von Reisenden ohne richterliche Überprüfung vor. Das Gesetz bestätigt Notstandsbefugnisse, die bisher nur bis Ende Mai 2016 zulässig wären. Die Regierung will die neuen Regeln noch vor der im Juni stattfindenden Fußball-Europameisterschaft durch das Parlament bringen.

Der Entwurf sieht vor, dass bei mutmaßlicher Terrorgefahr allein auf Basis einer Anordnung eines Präfekten, also des höchsten Vertreters der Zentralregierung in den Departements und Regionen, Hausdurchsuchungen, die Kontrolle von Autos oder des Gepäcks von Reisenden an Bahnhöfen veranlasst werden können. Der Einsatz moderner Abhörtechnik wie z. B. des sog. IMSI-Catchers, mit denen im räumlichen Umfeld von Verdächtigen sämtliche Handygespräche, E-Mails und sonstige elektronische Mobilkommunikation abgefangen werden kann, soll künftig durch jeden Staatsanwalt angeordnet werden können. Bisher war dies ein Privileg der von Weisungen der Regierung unabhängigen Untersuchungsrichter. Eine Regelung zum Schusswaffengebrauch würde PolizistInnen und GendarmInnen per Generalklausel unmittelbar nach Mordtaten erlauben, z. B. flüchtende GewalttäterInnen gezielt unter Feuer zu nehmen.

Die Sicherheitsbehörden zählen in Frankreich Anfang 2016 8520 „radikalisierte Personen“, was gegenüber März 2015 mehr als eine Verdoppelung ist. Besonders viele Verdächtige werden im Großraum Paris und im Südosten des Landes lokalisiert, wo überdurchschnittlich viele Nachkommen von Einwandernden aus dem Maghreb leben. Die Regierung schätzte, dass 605 Menschen aus Frankreich sich im Irak und in Syrien als „freiwillige Kämpfende“ verdingt haben. 738 weitere zumeist junge Männer wollten in die Kriegsgebiete aufbrechen, 275 seien 2015 vor der Ausreise gestoppt worden. Das neue Gesetz sieht vor, Rückkehrer aus Syrien präventiv auch dann unter Hausarrest zu stellen, wenn keine konkreten Beweise gegen die verdächtige Person vorliegen.

Premierminister Manuel Valls erklärte, die Terrorgefahr in Frankreich sei „so hoch wie nie zuvor“. Deshalb hatte die Regierung eine erneute Verlängerung des Notstands um 3 Monate bis Ende Mai 2016 beantragt. Menschenrechtsorganisationen und Richterverbände warnen, die neuen Regelungen bedrohten Grundrechte und schwächten die richterliche Kontrolle von Polizei und Geheimdiensten. Der Generalsekretär des Europa-Rats, der Norweger Thorbjorn Jagland, hatte im Januar 2016 in einem Schreiben an Staatspräsident Francois Hollande den Respekt für „fundamentale Freiheiten“ angemahnt (Wernicke, Normalzustand Ausnahme, SZ 04.02.2016, 6).

Frankreich

Geheimdienstgesetz durchgewunken

Der französische Geheimdienst will Seekabel oder Internetknotenpunkte praktisch ohne Einschränkungen anzapfen. Der französische Senat hat noch vor den Terroranschlägen im November in der Nacht vom 27. auf den 28.10.2015 zwei nachträgliche Ergänzungen eines im Juni verabschiedeten Überwachungsgesetzes verabschiedet, die Frankreichs Geheimdienst weitreichenden Zugriff auf internationale Datenströme ermöglichen. Bevor die Gesetzesänderung in Kraft treten kann, müssen sich der Senat und die Nationalversammlung als zweite Kammer des Parlaments noch auf eine gemeinsame Version verständigen.

Die zwei Klauseln hatte der Verfassungsrat für nicht verfassungskonform erklärt und aus dem ursprünglichen Gesetzentwurf gestrichen. Mit der Neuvorlage als Gesetzesänderung aus dem Parlament enthebt sich die Regierung der Pflicht, den Vorschlag erneut dem Verfassungsrat vorzulegen.

In einer Nachtsitzung hatte Berichterstatter Philippe Bas, unterstützt vom Vertreter des französischen Verteidigungsministeriums, die beiden knappen Paragraphen durch die Abstimmung gebracht. Abgefischte Kommunikation zwischen FranzosInnen solle gelöscht werden, versichert Bas. Bei „gemischten Datensätzen“ werde die laut dem neuen Gesetz einzurichtende Kontrollkommission CNCTR aktiv.

Kritiker halten die Schutzvorkehrungen im Gesetz für völlig unzureichend. Französische BürgerInnen, die ihre Kommunikation über ausländische Server abwickeln, seien nicht geschützt, kritisiert etwa die Organisation La Quadrature du Net. Ein besonderer Schutz für JournalistInnen, AnwältInnen oder Priester, die im Ausland arbeiten oder auch nur auf Reisen sind, sei überdies nicht möglich, meint der sozialistische Verteidigungsminister Jean-Yves Le Drian. Eine Journalistengruppe hat bereits Klage gegen das im Juni 2015 verabschiedete Gesetz beim Europäischen Gerichtshof für Menschenrechte eingelegt (Ermert, Frankreichs Senat winkt Carte Blanche für Geheimdienst durch, www.heise.de 28.10.2015).

Belgien

Gericht verbietet Cookie – Facebook geifert zurück

Knapp einen Monat nachdem es Facebook von einem belgischen Gericht in Brüssel am 09.11.2015 untersagt wurde, Daten über Nicht-Mitglieder zu sammeln, hat das Netzwerk angekündigt, diese fortan auszusperren. Nicht-Mitglieder könnten nicht länger auf öffentliche Facebook-Seiten, sog. Fanpages, von Unternehmen oder Organisationen zugreifen. Das sei die einzige Möglichkeit, Sicherheit zu gewährleisten. Außerdem wolle das Unternehmen auf das zuvor kritisierte „datr“-Cookie verzichten. Bislang gilt diese Maßnahme nur in Belgien, aber andere Länder dürften das

aufmerksam beobachten. Bei dem vor dem deutschen Bundesverwaltungsgericht anhängigen Verfahren zur Untersagung von Facebook-Fanpages durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) geht es auch um die Profilierungsmöglichkeit mithilfe dieses Cookies. Die Rechtsgrundlagen der belgischen Entscheidung gehen letztlich auf europäisches Recht zurück. Die Datenschutzbehörden stören sich daran, dass der Cookie für zwei Jahre auf dem Computer bleibt, z. B. auch wenn eine NutzerIn ihr Facebook-Konto deaktiviert.

Das belgische Gericht hatte entschieden, dass Facebook keine Daten von Nicht-Mitgliedern sammeln dürfe. Personenbezogene Daten dürften nur nach eindeutiger Zustimmung der Betroffenen aufgezeichnet werden. Wenn Facebook nicht innerhalb von 48 Stunden reagiere, werde eine Strafe in Höhe von 250.000 Euro pro Tag fällig. Das Gericht störte sich vor allem an dem „datr“-Cookie, das Informationen über alle Besuchenden von Seiten auf Facebook oder anderen Seiten mit einem „Like“-Button sammelt. Auch Nicht-Mitglieder bekommen das Cookie installiert. Dank der Facebook-Buttons auf anderen Seiten können die Betreiber des Netzwerks so auch Nicht-Mitglieder auf ihrem Weg durchs Netz verfolgen. Der Sicherheitschef von Facebook Alex Stamos rechtfertigte das „datr“-Cookie mit der Notwendigkeit falsche Profile herauszufiltern und Cyber-Attacken zu verhindern. Wenn etwa ein Web-Browser binnen 5 Minuten hundert Seiten besuche, sei das ein klares Zeichen dafür, dass der Computer wohl von Online-Kriminellen gekapert worden sei. Die Daten, die das Cookie sammele, würden nicht einzelnen Personen zugeschrieben und könnten auch nicht mit ihnen in Verbindung gebracht werden.

Willem Debeuckelaere, der Chef der belgischen Datenschutzbehörde, zeigte sich verärgert über Facebooks Reaktion auf das Gerichtsurteil: „Wir haben verlangt, dass sie aufhören, Nicht-Mitglieder zu verfolgen. Punkt.“ Stattdessen sehe es danach aus, dass Facebook ein Spiel spiele, um die Datenschützer in die Ecke zu drängen und als die Bösen darzustellen, die Informationen blockierten. Das Verhalten grenze an Erpressung. Facebook wehrte sich gegen diesen Vorwurf mit der Behauptung, es gebe keine andere Möglichkeit, als den Zugang zu sperren (Holland, Belgien: Facebook blockiert für Nicht-Mitglieder, www.heise.de 03.12.2015; Belgisches Gericht: Facebook darf keine Daten von Nicht-Mitgliedern sammeln, www.heise.de 09.11.2015).

Großbritannien

Sexuell aktive verdeckte Ermittler

Verdeckte Ermittler von Scotland Yard sind im Zuge ihrer Ermittlungen sexuelle Beziehungen zu Frauen eingegangen. Die Polizeibehörde entschuldigte sich am 20.11.2015 für das „komplett inakzeptable“ Verhalten einiger ihrer Mitarbeiter. Sie hätten versucht, in Protestgruppen hineinzukommen, indem sie intime Beziehungen zu weiblichen Mitgliedern eingegangen seien. Diese sexuellen Beziehungen seien „beleidigend, hinterlistig, manipulativ und falsch“ gewesen. Die Entschuldigung war Teil einer außergerichtlichen Einigung mit sieben Frauen (Hinterlistige Ermittler, SZ 21./22.11.2015, 12).

Großbritannien

Geheimdienste erhalten mehr Befugnisse zur Internetüberwachung

Die britische Innenministerin Theresa May stellte am 04.11.2015 eine Gesetzesinitiative im Parlament vor, mit der eine Vorratsspeicherung von Telekommunikationsdaten noch umfassender ausfallen würde als die bisherige Regelung des „Data Retention and Investigatory Powers Act“ (DRIPA), die der britische High Court am 17.07.2015 wegen mangelnder Bestimmtheit für unzulässig erklärte und nur noch übergangsweise in Kraft ließ. Die Regierung in London will Provider nun dazu verpflichten, neben den gängigerweise eingeschlossenen Verbindungs- und Standortdaten auch Inhalte anlasslos zu speichern. Die Zugangsanbieter sollen ferner Informationen über besuchte Webseiten sowie die E-Mail- oder die Chat-Kommunikation ein Jahr auf Vorrat einlagern müssen. Das Ministerium wies darauf hin, dass nicht die komplette Browser-Historie gespeichert werden soll, obwohl die Geheimdienste genau dies gefordert hatten.

Es war wohl kein Zufall, dass kurz vor der Präsentation des Gesetzentwurfes der britische Geheimdienst Government Communications Headquarters (GCHQ) just zum Start des Bond-Films „Spectre“ eine PR-Offensive startete und erstmals JournalistInnen Zugang zum Hauptquartier in Cheltenham gewährte.

2014 hatte die damalige konservativ-liberale Koalition unter Premierminister David Cameron nach dem Urteil des Europäischen Gerichtshofs (EuGH) zur Vorratsdatenspeicherung vom 08.04.2014 zunächst ein „Notstandsgesetz“ zur Vorratsdatenspeicherung verabschiedet und später eine dauerhafte Lösung angedeutet, mit der auch Verschlüsselung umgangen werden soll. Das Gesetz sorgte nicht nur dafür, das die vom EuGH gekippte Vorratsdatenspeicherung beibehalten wurde, sondern führte bereits die Überwachungsersuchen an ausländische Unternehmen ein. Damals war festgelegt worden, dass die Regelung im Jahr 2016 ausläuft. Nach den Neuwahlen im Mai 2015 kündigte Königin Elisabeth II. einen entsprechenden Vorstoß an, ohne Details für die „Snoopers‘ Charter“ zu nennen.

Der High Court hatte im Juli unter anderem gerügt, dass Polizeien, Geheimdienste und andere Behörden bislang ohne Richtergenehmigung auf die Daten zugreifen dürften. Hier will die Regierung nachbessern.

Selbst erzkonservativen Politikern wie dem früheren Staatsminister David Davis geht der neue Vorstoß generell zu weit. Ihm zufolge gibt es keine Nachweise dafür, dass die begehrten Telekommunikationsdaten ein Jahr lang im Interesse der Strafverfolgung aufbewahrt werden müssen. Der Liberale Nick Clegg, der als Camerons Vize eine Vorratsdatenspeicherung einschließlich von Kommunikationsinhalten noch verhindert hatte und mittlerweile nicht mehr in der Regierung sitzt, hatte jüngst gewarnt, dass Großbritannien mit einer massiven Datenbank zu den Browsing-, Mail- und Chatgewohnheiten der Nut-

zenden viel zu tief in deren Grundrechte einschneiden und einen „besorgniserregenden internationalen Präzedenzfall“ schaffen würde. Dem gegenüber meinte der Schatten-Innenminister von Labour, Andy Burnham, es gebe eine breite Akzeptanz, dass ein neues Gesetz verabschiedet werden müsse, damit das Land effektiv gegen Terroristen, Pädophile und andere Kriminelle vorgehen könne, und warnte vor einer „überhysterischen Reaktion“ auf Mays Pläne. Die Direktorin der Bürger- und Menschenrechtsorganisation Liberty, Shami Chakrabati, meinte: „Es ist der typische Tanz des Innenministeriums, erst extrem weitreichende Kompetenzen zu verlangen, damit selbst kleinste Konzessionen als vernünftig erscheinen.“

Apple-Chef Tim Cook hat bereits Anfang November 2015 öffentlich gegen den Gesetzesentwurf Stellung bezogen. Im Dezember legte der Konzern mit einer förmlichen Stellungnahme nach: Die Integration von Hintertüren und Überwachungsmöglichkeiten würde die in Apple-Produkte eingebauten Schutzsysteme schwächen und alle KundInnen in Gefahr bringen. „Ein Schlüssel unter der Fußmatte steht nicht nur den Guten zur Verfügung, die Bösen finden diesen auch“. Auch die klügsten Köpfe könnten die Gesetze der Mathematik nicht ändern. „Jeder Prozess, der die mathematischen Modelle zum Schutz von Nutzerdaten schwächt, wird automatisch das gesamte Schutzsystem schwächen“. Cook gab sich optimistisch: „Wenn sich die Öffentlichkeit engagiert, wenn sich die Presse stark und ausdauernd engagiert, dann wird es den Menschen bewusst werden, was gebraucht wird. Verschlüsselungen dürfen nicht geschwächt werden. Sie müssen gestärkt werden.“ Datenschutz und nationale Sicherheit schlössen sich nicht aus. Apples Kommunikationsdienste iMessage und FaceTime setzen auf Ende-zu-Ende-Verschlüsselung. Das Unternehmen betont, es könne den Inhalt der Nachrichten nicht einsehen. Auf richterliche Anfrage stellt Apple nach eigener Angabe aber Metadaten zu den Kommunikationsvorgängen bereit. Staatliche Stellen können mit einem richterlichen Beschluss außerdem den Zugriff auf bestimmte iCloud-Daten anfordern, darunter auch das iCloud-Backup. Es könne neben App-Daten auch „iMessage, SMS- und MMS-Nachrichten sowie Voicemail-Mitteilungen“ beinhalten, so Apple in den Legal Process Guidelines für Strafverfolgungsbehörden.

Laut Apple droht das geplante Gesetz außerdem, nicht in Großbritannien ansässige Konzerne dazu zu „zwingen, die Gesetze ihrer Heimatländer zu brechen“, wenn sie Informationen zu ihren Nutzern auf eine staatliche Anfrage hin herausgeben sollen. Dies würde den IT-Sektor lähmen und „ernste internationale Konflikte“ auslösen: „Es könnte für einen deutschen Nutzer bedeuten, dass seine Daten auf Anordnung des britischen Staates von einer irischen Firma gehackt werden“, so der Konzern, der sein Europa-Geschäft über eine irische Tochterfirma abwickelt.

Kritik kam auch von Yahoo. Der mit dem Gesetzesentwurf befasste Parlamentsausschuss plante für Februar 2016 die Erstellung eines Berichts (Krempl, Britischer High Court kippt nationale Vorratsdatenspeicherung, www.heise.de 17.07.2015; Krempl, Großbritannien plant Vorratsspeicherung auch von Inhaltsdaten, www.heise.de 30.10.2015, Zaschke, Lizenz zum Speichern, SZ 03.11.2015, 7; Becker, Apple protestiert gegen britisches Netzüberwachungsgesetz, www.heise.de 22.12.2015).

USA

Gag Order nach National Security Letter aufgehoben

Nicholas Merrill, heute 42 Jahre alt, betrieb 2004 eine Webhosting-Firma namens Calyx Internet Access, die zahlenden KundInnen Speicherplatz zur Verfügung stellte, um ihre Webseite ins Netz zu stellen. Damals riefen Agenten des Federal Bureau of Investigation (FBI) bei Merrill an und teilten ihm mit, dass sie einen Brief für ihn hätten. Keine zwei Stunden später klopfte das FBI an seine Tür und forderte Informationen über einen von Merrills Kunden an. Anders als üblich, enthielt dieser Brief keine Unterschrift eines Richters, der die Rechtmäßigkeit des Informationsverlangens hätte überprüfen können.

Bei dem Brief handelte es sich um einen sogenannten „National Security Letter“ (NSL). Nach den Anschlägen im September 2001 bekamen US-Behörden mit dem „Patriot Act“ weitreichende Befugnisse, um Terroristen aufzuspüren, bevor diese ein Attentat durchführen können. Diese Befugnisse umfassten auch die Art und Weise, wie NSL eingesetzt werden dürfen. Gemäß dem Patriot Act ist kein konkreter Tatverdacht für das Verlangen nötig; die „Relevanz“ für eine Ermittlung, um Terroranschläge zu verhindern, reicht aus. Einer von Präsident Obama eingesetzten Expertenkommission zufolge verschickt das FBI 60 NSL pro Tag. Zusammen mit dem Brief erhielt Merrill eine „Gag Order“, womit dem Auskunftspflichtigen untersagt wird, über den Erhalt des Briefes und dessen Inhalt zu sprechen. Heute meinte Marrill: „Es war eine furchtbare Zeit. Ich hätte nie gedacht, dass dieser Fall mich ein Viertel meines Lebens beschäftigten würde.“

Im August 2015 entschied ein US-Richter, dass die Regierung nicht das Recht hat, Menschen auf unbestimmte Zeit zum Schweigen zu verdonnern. Der Regierung wurden 90 Tage eingeräumt, um gegen diese Entscheidung Einspruch einzulegen. Nach Fristablauf ohne Rechtsmittel ist der Maulkorb fort. Es ist das erste Mal, dass eine „Gag Order“ komplett annuliert wurde.

Merrill darf nun reden und die Anfrage veröffentlichen: Das FBI verlangte Auskunft zu 17 Punkten, darunter sämtliche URL-Adressen, die einem von Merrills Firma gehosteten Nutzerkonto zugewiesen waren, alle von dem Kunden getätigten Online-Käufe der vergangenen 180 Tage und sämtliche Funkzellen, in denen dieser eingeloggt war.

Gemäß der Interpretation von Merrill und seinen Verteidigern von der Yale University will das FBI mit derartigen URL-Anfragen den gesamten Suchlauf im Internet nachvollziehen. Außerdem sind gemäß dem NSL alle IP-Adresssen preiszugeben, mit denen ein Nutzender in Kontakt stand. Merrill: „Diese Daten geben die intimsten Daten über unser Leben preis: unsere politischen Aktivitäten, religiösen Überzeugungen, unsere Kontakte und auch unsere Gedanken.“

Merrill hatte über die Jahre bereits Teilsiege errungen. So darf er seit 2010 öffentlich sagen, eine FBI-Anfrage er-

halten zu haben. Die Klage reichte er als „John Doe" ein, was dem deutschen „Max Mustermann" entspricht. Bei seinen eigenen Gerichtsterminen durfte er nur im Publikum sitzen. Seiner Freundin durfte er nicht erzählen, dass er sich mit Anwälten traf. Die Anwälte selbst wussten nicht, ob sie Merrill unterstützen dürfen, so Jameel Jaffer von der Bürgerrechtsgruppe ACLU: „Wir hatten keine Antwort, da wir bis dato keinen NSL zu Gesicht bekommen hatten." Merrill betreibt schon seit längerer Zeit keine Firma für Webhosting mehr. Stattdessen will er Menschen dazu bringen, ihre Online-Kommunikation vor Angreifern abzusichern (Tandriverdi, Wie das FBI einen Internet-Unternehmer zum Schweigen bringt, www.sueddeutsche.de 23.09.2015; Tandriverdi, SZ 02.12.2015, 19).

USA

Obama-Regierung verzichtet auf Backdoors

Die US-amerikanische Regierung verzichtet darauf, sich per Gesetz Zugriff auf verschlüsselte Daten von Internet- und Handynutzern zu sichern. Dieser Entscheidung von Präsident Barack Obama war ein monatelanger Streit zwischen den größten Technikkonzernen, DatenschützerInnen und VerschlüsselungsexpertInnen auf der einen Seite und den US-Behörden auf der anderen vorausgegangen. Apple, Google, Facebook und andere Firmen zogen nun die Regierung wenigstens zum Teil auf ihre Seite.

Ursprünglich hatte die US-Regierung von den Firmen verlangt, dass sie für verschlüsselte Geräte wie zum Beispiel iPhones eine Art Generalschlüssel bereithalten. Mit dem sollten dann Behörden wie die Bundespolizei FBI die Systeme der Nutzenden knacken können, sofern Ermittlungen dies verlangt hätten. Immer mehr Alltagsgeräte und Software wie Telefone, Tabletcomputer oder auch Whatsapp verschlüsseln standardmäßig zumindest ihren internen Speicher. Immer öfter können die Firmen die Daten ihrer KundInnen deshalb nicht durchsuchen, selbst dann nicht, wenn ihnen ein Durchsuchungsbefehl präsentiert wird.

Für die Obama-Regierung soll nun die Sorge ausschlaggebend gewesen sein, dass von den Technik-Konzernen eingebaute Hintertürchen in die Verschlüsselungstechnik nicht nur von den eigenen Behörden, sondern auch von fremden Spionen genützt werden könnten. Neben dem technischen Argument sprach offenbar auch eine politische Abwägung für die Zurückhaltung der Behörden. Nachdem auch Chinesen und Russen von US-amerikanischen IT-Konzernen verlangen, Hintertüren in ihre Geräte einzubauen, wollte das Weiße Haus wohl auch ein außenpolitisches Signal geben (vgl. in diesem Heft S. 35).

In den amerikanischen Sicherheitsbehörden stieß die Regierungsentscheidung auf Ablehnung. Insbesondere das FBI befürchtet, dass es künftig nicht mehr effizient ermitteln könne. Die Geheimdienste wie die umstrittene National Security Agency (NSA) hielten sich hingegen in der Debatte auffallend zurück. Sie sind offenbar weniger auf das Entgegenkommen der Konzerne angewiesen, weil sie über technisch stärkere Möglichkeiten verfügen als klassische Behörden und auch verschlüsselte Daten knacken können (Boie, Obama will Zugriff auf Handy-Daten erschweren, SZ 13.10.2015, 1 = www.sueddeutsche.de 12.10.2015).

USA

Clappers Privataccount geknackt

Der US-Geheimdienstkoordinator James Clapper hat eingestanden, dass seine privaten Onlinekonten gehackt worden sind. Ein Jugendlicher mit dem Pseudonym «Cracka» bekannte sich zum Hackerangriff auf Clappers Internet- und Telefonkonto. Gemäß Presseberichten gelang es dem Hacker, Anrufe an Clappers Nummer zur propalästinensischen Bewegung Free Palestine Movement umzuleiten. Auch habe er es geschafft, in ein Yahoo-Konto von Clappers Ehefrau einzudringen. Der Hacker soll einer Gruppe angehören, die bereits in einen Cyberangriff auf das private Email-Konto des CIA-Direktors John Brennan verwickelt war. Brennan hatte empört auf den Angriff und Medienberichte darüber reagiert («Cracka» hackt Onlinekonten von US-Geheimdienst-Koordinator Clapper, http://www.watson.ch 13.01.2016).

USA

Wählerverzeichnis war öffentlich zugänglich

Über eine fehlkonfigurierte Datenbank waren in den USA Daten von 191 Mio. WählerInnen öffentlich zugänglich. In den USA muss sich jede Person registrieren lassen, um wählen zu dürfen, und wird dafür in einer Datenbank erfasst. Die dort abgelegten Informationen enthalten Angaben zu Vor- und Zunamen, Anschrift, Festnetznummer, Geburtsdatum, Geschlecht und Ethnizität. Außerdem enthalten sie Informationen darüber, zu welchen der Wahlen die betreffende Person seit 2000 gegangen ist und gegebenenfalls, welcher Partei sie angehören. Das erlaubt Rückschlüsse auf künftige Wahlgänge und Präferenzen.

Der texanische Sicherheitsspezialist Chris Vickory stellte fest, dass die Daten öffentlich zugänglich sind. Die Echtheit der Informationen verifizierte er anhand seines eigenen Namens. Er konnte zunächst nicht feststellen, wem der Server gehört, und hat das FBI sowie den Generalbundesanwalt von Kalifornien eingeschaltet. Schließlich sind auch die Daten von 17 Mio. Menschen aus Kalifornien betroffen. Außerdem macht der Staat als einer von wenigen Bundesstaaten die Wählerdaten nicht offen zugänglich.

Einige Staaten legen die Daten ihrer registrierten Wähler offen. In der hier bloßgelegten Datenbank waren sie aber vollständig und besonders konzentriert zu finden. Die Daten wären für Kriminelle geeignet gewesen, Wohnorte von PolizistInnen aufzuspüren oder sie als Ausgangsbasis für Online-Betrug zu nutzen. Wer Zugang zu der Datenbank genommen hat, blieb unklar (Kramer, Daten von 191 Millionen US-Wählern offengelegt, www.heise.de 29.12.2015).

USA

Prügler fordert Millionen Schmerzensgeld

Der 32-jährige Benjamin Goldenversucht, wegen einer Persönlichkeits-

verletzung mehrfacher Millionär zu werden, nachdem er von seinem Prügelopfer im Internet bloßgestellt wurde. Im Oktober 2015 stieg er betrunken in ein Auto des Fahrdienstes Uber; er stritt mit dem Fahrer Edward Caban über den korrekten Weg und wurde hinausgeworfen. Er verprügelte daraufhin seinen Chauffeur, zog ihn an den Haaren, beschimpfte ihn und verließ das Auto erst, als sich Caban mit Pfefferspray wehrte. Eine im Fahrzeug angebrachte Kamera hatte den Vorfall aufgezeichnet, Caban überließ das Video der Polizei und stellte es anschließend ins Internet. Dazu verklagte er Golden trotz dessen tränenreicher Entschuldigung im Fernsehen („Das bin nicht ich. Ich schäme mich. Ich habe Mist gebaut.“) auf 1,6 Mio. Dollar Schmerzensgeld.

Golden setzte zur Gegenwehr an und verklagte den Fahrer auf fünf Millionen Dollar Schmerzensgeld. Das Video, mittlerweile millionenfach im Internet angeklickt, sei ohne seine Zustimmung erstellt und veröffentlicht worden. Es habe bei ihm für emotionale Schmerzen, Demütigungen und Angstzustände gesorgt, zudem habe er deshalb seine gut bezahlte Anstellung verloren und seitdem keinen Job mehr gefunden. Außerdem habe ihn Caban in Gefahr gebracht, weil er ihn aus dem Auto geworfen habe. In der Klageschrift heißt es: „Golden wusste nicht, wo er sich befand und musste deshalb um seine Sicherheit fürchten“.

Es gibt in den USA einen kompletten Wirtschaftszweig, der sich ausschließlich mit derartigen Klagen beschäftigt. AnwältInnen diskutieren nun über die Erfolgsaussichten dieses Falles, weil dieser weitere Kreise ziehen könnte: Im Bundesstaat Kalifornien ist es eine Straftat, eine vertrauliche Unterhaltung an einem privaten Ort zu belauschen oder ohne die Zustimmung aller GesprächspartnerInnen aufzuzeichnen.

Die zentrale rechtliche Frage ist also nicht, ob es klug und legitim war, die Aufnahmen ins Internet zu stellen. Vielmehr kommt es darauf an, ob das Auto eines Uber-Fahrers, der nicht Angestellter des Unternehmens ist, ein öffentlicher oder privater Ort ist. Ein Bus etwa gilt in Kalifornien als öffentlich, ein Privatauto nicht unbedingt. Deshalb werden Golden Chancen eingeräumt, mit seiner Klage erfolgreich zu sein. Er wäre dann Millionär, weil er dabei gefilmt worden ist, wie er jemanden verprügelt hat (Schmieder, Vom Prügler zum Millionär, SZ 25.01.2016, S. 17).

USA

Versteckte Kamera in Airbnb-Wohnung

Yvonne Schumacher, eine deutsche Touristin, reichte im Dezember 2015 gegen das Wohnungsvermittlungsportal Airbnb und die an sie vermittelten Vermieter Klage ein, weil sie von einer versteckt installierten Kamera erfasst worden ist. Sie beschreibt, dass sie nachts auf die Toilette gehen wollte, doch das Bad war ihr zu verdreckt. Sie benutzte also ein anderes Badezimmer und ging nackt durch die Wohnung, vorbei am Wohnzimmer. Ihr Anwalt Michael Jackson erläuterte: „Dabei ist sie genau durch das Blickfeld einer Kamera gelaufen“. Schumacher war mit einem Mann zu Gast, der aus einem der Regale eine Lichtquelle wahrnahm und so die Kamera fand. Er arbeite im IT-Umfeld, kenne sich mit technischen Geräten also aus und habe so feststellen können, dass die Kamera laufe. Sie sei aus der Ferne steuerbar und auch in der Lage, Töne aufzunehmen. Erfasst wurden also möglicherweise auch jene Privatgespräche, die Schumacher und ihre Begleitung in den vorangegangenen Tagen im Wohnzimmer geführt hatten.

Der Anwalt kündigte an, dass man während des Prozesses zeigen werde, dass die Kamera aktiv von den Vermietern genutzt wurde. „Das war eine grobe Verletzung der Privatsphäre.“ Jackson sagte, Airbnb habe den Vermietern auch nach Melden des Vorfalls erlaubt, die Wohnung zu vermieten. Der Airbnb-Sprecher verneint das. Der Anwalt meinte, seine Mandantin sei schockiert und fühle sich gedemütigt. Sie habe Angst, dass nun Nacktfotos von ihr im Internet landen oder als Druckmittel eingesetzt werden könnten. Airbnb stelle sich gerne als vertrauenswürdiger Makler dar, so Jackson: „Das stimmt natürlich nicht. Es gibt keine Sicherheitsvorkehrungen, um die Mieter zu schützen.“ In Hotels sei klar geregelt, dass sich in Zimmern keine Kameras befinden dürfen. In den USA aber würden sie in privaten Wohnungen oder Häusern, wie sie Airbnb vermittelt, immer häufiger eingesetzt.

Ein Sprecher von Airbnb erklärte, dass „über 65 Millionen Gäste positive, vertrauenswürdige Erfahrungen mit Airbnb“ gemacht hätten. Schumacher und die angebliche Spanner-Kamera sei ein „unglaublich seltener Fall“. Jedes Jahr würden zehntausende Vermietungen über die Plattform laufen, ohne dass Schäden auftreten. Das erfolgreiche Start-up Airbnb wird mit 25 Milliarden Dollar bewertet. Allerdings stand Airbnb in den vergangenen Jahren wiederholt in der Kritik. Mal wurden Wohnungen zerstört, mal haben Mieter die Wohnung als Set für einen Porno-Dreh verwendet. Anfang 2015 wurden mehrere Kameras in einer Airbnb-Wohnung in Kanada gefunden.

Jahrelang gab Airbnb in den Geschäftsbedingungen nicht an, dass Vermieter angeben müssen, ob sie Kameras in ihren Wohnungen installiert haben. Seit September 2014 besteht nun eine Anweisung, dass Vermieter Gäste auf Kameras hinzuweisen haben. AktivistInnen haben bereits angefangen, eine digitale Gegenwehr zu ermöglichen. Der Künstler Julian Oliver hat ein Programm geschrieben, das im lokalen Netzwerk nach Kameras sucht und diese automatisch aus dem Netzwerk wirft (Tandriverdi, Versteckte Kamera, SZ 14.01.2016, 17).

Brasilien

Gericht blockiert Whatsapp 14 Stunden lang

Am 17.12.2015 bestand für 14 Stunden in ganz Brasilien eine Sperre des Internetdienstes WhatsApp. Die Blockade war von einem Gericht in São Bernardo do Campo im Bundesstaat São Paulo für 48 Stunden angeordnet worden. Die Richterin Sandra Regina Nostre Marques hatte die Telefon- und Internetunternehmen dazu kurzfristig aufgefordert. Hintergrund ist ein Strafverfahren, in dem WhatsApp nicht kooperiert haben soll, bei dem es um die Herausgabe von Daten oder Chat-Protokollen zu mutmaßlich kriminellen Handlungen ging. Im Februar 2015 war eine vergleichbare landesweite Blockade noch von einer Berufungsinstanz zurückgewiesen worden. Damals

ging es laut Medienberichten um die Herausgabe von Daten im Zusammenhang mit einem Pädophilie-Fall. Der Richter des Gerichtshofs des Bundesstaates Sao Paulo Xavier de Souz hob die Entscheidung der Richterin im Rechtsmittelverfahren wieder auf und bezeichnete die Maßnahme als „unangemessen“. Eine Geldstrafe sei angebrachter als Dutzende Millionen an Nutzenden zu bestrafen. Kurz nach dieser Entscheidung funktionierte der Dienst wieder.

Mit Whatsapp können unter anderem kostenlos Nachrichten, Fotos, Videos und Sprachmitteilungen versendet werden. Facebook hatte den Dienst 2014 für 22 Milliarden Dollar gekauft. Der Chef von Facebook Mark Zuckerberg kritisierte die Blockade des Dienstes scharf: „Das ist ein trauriger Tag für Brasilien. Brasilien ist bisher ein Verbündeter gewesen bei der Schaffung eines offenen Internets.“ Es könne nicht sein, dass die Entscheidung einer Richterin „jede Person in Brasilien bestraft, die Whatsapp benutzt“. Diese forderte er auf, ihre Stimme zu erheben. Zuckerberg betonte, Datenschutz sei ein hohes Gut. Fraglich ist, ob Whatsapp wegen der verwendeten Verschlüsselungstechnik überhaupt in der Lage gewesen wäre, die geforderten Daten herauszugeben.

Die führenden Telefongesellschaften Vivo, Tim, Claro, und Oi hatten die gerichtliche Anordnung notgedrungen umgesetzt. Auch WLAN-Verbindungen waren betroffen. Mit der Blockade nutzte das Gericht technische Sperrmöglichkeiten in einer bisher beispiellosen Größenordnung, um Druck auf den Anbieter auszuüben, damit dieser Daten seiner Nutzenden herausgibt. Wenn sonst soziale Medien wie Twitter oder YouTube in manchen Ländern blockiert werden, geschieht dies eher, um den Zugang zu unliebsamen Inhalten oder Daten zu erschweren. Brasilien gilt als eines der Länder mit den meisten WhatsApp-Nutzenden. Laut dem US-Branchendienst TechCrunch beträgt ihre Zahl dort 93 Millionen. Weltweit sollen rund 900 Millionen Menschen WhatsApp nutzen.

Kurz vor dem Start der Blockade in der Nacht zum 17.12. wurden noch Nachrichten verschickt: „Auf Telegram ausweichen“. Der brasilianische Dienst Telegram funktioniert ähnlich wie Whatsapp. Mit einer Internetverbindung können kostenlos Nachrichten versendet werden. Telegram berichtete noch am gleichen Tag, dass man über 1,5 Mio. neue Nutzende gewonnen habe (Brasilien: Zuckerberg tobt wegen WhatsApp-Sperre, www.spiegel.de 17.12.2015; Zuckerberg tobt: Brasilien schaltet Wahtsapp ab, Kieler Nachrichten 18.12.2015, 6).

Pakistan

Regierung fordert erfolglos Vollzugriff auf Blackberry-Daten

Die pakistanische Regierung besteht nicht mehr auf einer Überwachung von Blackberry-Nutzerdaten. Sie hatte Zugriff auf Server des kanadischen Smartphone-Herstellers gefordert, weshalb Blackberry sich aus dem Land zurückziehen wollte. Die staatliche Telekommunikationsbehörde PTA hatte im Juli 2015 gefordert, Zugang zu den Blackberry Enterprise Servern (BES) zu erhalten, um die Überwachung zu erleichtern und um Zugriff auf den gesamten Datenverkehr zu erlangen, der über die BES läuft. Das schließt nicht nur Informationen über die Benutzenden selbst, sondern auch E-Mails und Kurznachrichten ein. Von dem Rückzug wären in Pakistan wohl weniger als 5.000 KundInnen betroffen gewesen. Die pakistanische Telekommunikationsbehörde hatte ihr Anliegen damit begründet, dass immer mehr Kriminelle auf sichere Kommunikation ausweichen würden. AnalystInnen entgegneten dem aber, dass die Regierung ihre Online-Überwachung in Wahrheit ausweite, um AktivistInnen, Politiker Innen und JournalistInnen ins Visier zu nehmen.

Auch Blackberry meinte, dass es Pakistans Regierung nicht um die öffentliche Sicherheit ging. Man habe sich bereit erklärt, Sicherheitsbehörden bei Ermittlungen zu helfen. Pakistan habe jedoch uneingeschränkten Zugang zu den Daten von BES-KundInnen gefordert. Dem Datenschutz müsse Vorrang eingeräumt werden. Dieses Prinzip werde man nicht aufgeben. Der Smartphone-Hersteller selbst hat keinen Zugriff auf die verschlüsselten Daten und lehnte es ab, sich Zugang zu verschaffen. Blackberry hatte angekündigt, sein Engagement in Pakistan bis Ende des Jahres 2015 zu beenden, falls die Regierung die Überwachungspläne nicht zurückziehe.

Mit ähnlichen Schwierigkeiten hatte Blackberry bereits in Indien, den Vereinigten Arabischen Emiraten, Saudi-Arabien und Indonesien zu kämpfen. Verantwortliche der Telekommunikationsbehörde PTA hatten argumentiert, dass sie nichts anderes verlangten als in anderen Ländern. So habe sich Blackberry etwa in Saudi-Arabien dem Ansinnen der Geheimdienste gebeugt (Kramer, Blackberry bleibt in Pakistan, www.heise.de 03.01.2016; Holland, Blackberry will Pakistan verlassen, www.heise.de 30.11.2015).

Hongkong

Kinderdaten von VTech geklaut

Bei einem Hack des Spielzeug- und Lernsoftware-Herstellers mit Sitz in Hongkong „VTech“, der auch auf dem deutschen Markt vertreten ist, haben Unbekannte rund 6,4 Millionen Profile mit Angaben u. a. zu Wohnadressen, Vornamen, Geburtstagen und Geschlecht von Kindern sowie 4,9 Millionen Konten von Eltern gehackt. Das Unternehmen erklärte, dass in Deutschland knapp 391.000 Eltern-Konten gehackt und rund 509.000 Kinder-Profile betroffen sind. Der Großteil des Datenlecks treffe die USA mit 2,2 Millionen Eltern- und fast 2,9 Millionen Kinder-Accounts. Mehrere Gigabyte der erbeuteten Daten wurden ins Internet gestellt. VTech vertreibt unter anderem Spiel-Computer und Lern-Software.

Laut einer E-Mail, die VTech Ende November an betroffene KundInnen verschickte, wurde der Angriff von der Firma am 14.11.2015 festgestellt. Die Hacker hatten sich demnach über den Download-Manager des App Stores Zugang zur Kundendatenbank verschafft. Die enthalte Namen, E-Mail-Adressen, verschlüsselte Passwörter, Sicherheitsabfragen und -Antworten zur Kennwortwiederherstellung, IP-Adressen sowie Postanschriften und Download-Chroniken. Daten zu Bankverbindungen und Kreditkarten sowie persönliche Identifikationsnummern wurden laut Hersteller

nicht erbeutet. VTech erklärte weiter, dass ein Medienbericht, wonach die Hacker auch Fotos von Kindern und Protokolle von Chats mit ihren Eltern abgreifen konnten, geprüft werde. Man könne das zunächst nicht bestätigen. Auf jeden Fall seien die Bilder per Verschlüsselung geschützt.

Gemäß der US-Internetseite Motherboard erfolgte der Angriff mit einer seit Jahren bekannten Masche, bei der Datenbanken mit gezielt fehlerhaften Anfragen dazu gebracht werden, den Zugriff freizugeben. Die Passwörter waren zwar verschlüsselt, jedoch mit einem Verfahren, das als relativ leicht zu knacken gilt. Nach Ansicht von Larry Salibra, Gründer und Chef einer Firma für Software-Fehlertests, wurden im Fall von VTech einfachste Grundregeln der IT-Sicherheit missachtet: „Das scheint ein Trend zu sein: Hardware-Hersteller legen keinen großen Wert auf Software-Fähigkeiten, wahrscheinlich, weil sie keinen unmittelbaren positiven Effekt auf ihr Geschäft sehen.“ Das gelte aber nur solange, bis etwas wie ein Hackerangriff passiere.

Die Webseite „Have I been pwned“ des Sicherheitsforschers Troy Hunt ermöglichte es den KundInnen zu prüfen, ob auch ihre Daten den Hackern in die Hände gefallen sind, indem sie die für VTech-Dienste genutzte E-Mail-Adresse oder der Benutzername in das Suchfeld eingeben. Die Datenbank der Webseite enthält zudem Einträge zu weiteren großen Datenlecks von Diensten wie Amazon, Ashley Madison, Snapchat, Patreon oder Vodafone.

In den USA haben mindestens zwei Bundesstaaten wegen des Vorfalls Ermittlungen aufgenommen. Die Datenpanne des Hongkonger Unternehmens gehört zu den größten bisher bekannt gewordenen. Im Februar 2015 waren der US-Versicherung Anthem 80 Millionen Datensätze gestohlen worden. Dem Seitensprung-Portal Ashley Madison kamen im Juli 2015 37 Millionen Datensätze abhanden (Datenleck bei Spielzeug-Firma VTech größer als gedacht, www.heise.de 02.12.2015; Martin-Jung, Kinder-Daten geklaut, SZ 01.12.2015, 26; Webseite zeigt von VTech-Hack betroffene Nutzerkonten, www.heise.de/security/ 30.11.2015, Radke, VTech-Hack: Knapp 5 Millionen Daten von Kunden und Kindern erbeutet, www.heise.de 28.11.2015).

China

Umstrittenes Anti-Terror-Gesetz verabschiedet

Die chinesische Regierung hat ein „Anti-Terror-Gesetz“ verabschiedet, das den Behörden Zugriff auf verschlüsselte Daten ausländischer Unternehmen ermöglicht. Die staatliche Nachrichtenagentur Xinhua teilte mit, dass der Ständige Ausschuss des Nationalen Volkskongresses dem „ersten Anti-Terror-Gesetz des Landes“ und dem Ausbau staatlicher Überwachungsmechanismen zugestimmt hat.

Das Gesetz zur nationalen Sicherheit verlangt, dass alle wichtigen Infrastrukturnetze und Informationssysteme „sicher und kontrollierbar“ sind. Das bedeutet, dass Technologiefirmen der chinesischen Regierung gegebenenfalls Zugang zur ihren Produkten sowie zu Kodierungsschlüsseln geben müssen. Dies wurde nicht nur von westlichen Wirtschaftsverbänden kritisiert. US-Präsident Barack Obama trug im Vorfeld in Gesprächen mit seinem chinesischen Kollegen Xi Jinping Bedenken vor: „Wir haben sehr deutlich gemacht, dass sie das ändern müssen, wenn sie mit den USA Geschäfte machen wollen.“ Der Gesetzentwurf zwinge alle ausländischen Unternehmen, der chinesischen Regierung Mechanismen an die Hand zu geben, um ihre KundInnen auszuspionieren, bemängelte der US-Präsident: „Sie können sich vorstellen, dass die Konzerne dazu nicht bereit sein werden.“ Aus Sicht der USA setze die Volksrepublik ausländische Unternehmen durch unfaire Maßnahmen der Aufsichtsbehörden unter Druck. China könne damit in die Privatsphäre von Verbrauchern eindringen. Das Gesetz behindere die freie Meinungsäußerung sowie den US-Handel mit China. Das chinesische Außenministerium hingegen warf den USA unrechtmäßige Einmischung vor und teilte mit, Technologiefirmen hätten nichts zu befürchten.

Obamas eigene Behörden, namentlich das FBI und die NSA, wollen solche Hintertüren in den Produkten der US-Firmen ebenfalls haben. Und die US-Unternehmen denken dabei nicht nur an die eigene Regierung, sondern eben auch an die chinesische. So hatte Yahoos Sicherheitschef den NSA-Direktor Michael Rogers gefragt, ob er die eigenen Sicherheitsvorkehrungen auch für andere Regierungen aushebeln soll, wenn die ein entsprechendes Gesetz beschließen. Rogers gab darauf die Antwort: „Ich denke, wir können uns da durcharbeiten“.

Ein Mitglied des Rechtsausschusses des Parlaments sagte, China hole mit dem Gesetz lediglich nach, was westliche Staaten schon getan hätten – nämlich IT-Firmen zu bitten, bei der Bekämpfung des Terrorismus zu helfen. Die normale Arbeit der Unternehmen sei davon nicht berührt. Sie hätten auch nichts zu befürchten hinsichtlich der Installation sogenannter Hintertüren für den Zugang zu Daten oder der Verletzung von Urheberrechten.

„Die chinesische Regierung trifft konkrete Maßnahmen, um ihr Volk und auch normale Amerikaner zu schützen, die etwa Weihnachten im Pekinger Sanlitun-Viertel verbringen“, hieß es auf einer Nachrichtenseite der staatlichen Nachrichtenagentur Xinhua. Die USA erwiesen sich als Meister der doppelten Standards, hätten sie doch selbst längst vergleichbare Gesetze verabschiedet. Die Polizei in der chinesischen Hauptstadt hatte den geschäftigen Amüsier- und Einkaufsbezirk kurz vorher nach einer Sicherheitswarnung abgeriegelt. Das neue Gesetz eröffnet auch rechtlich die Möglichkeit, dass die chinesischen Streitkräfte an Anti-Terroreinsätzen im Ausland teilnehmen. Den Medien wird die Beschränkung auferlegt, dass sie über Details von Terroranschlägen nicht berichten dürfen. Begründet wird dies damit, dass Nachahmungstäter nicht durch die Berichte angestiftet werden sollen.

China sieht sich immer wieder mit Protesten und Aufständen des Turkvolkes der Uighuren in der westlichen Region Xinjiang konfrontiert. Die Regierung macht muslimische Extremisten dafür verantwortlich. MenschenrechtlerInnen sehen den Anlass für die dortigen Unruhen in der Diskriminierung der Uighuren (China verabschiedet umstrittenes Anti-Terror-Gesetz, www.zeit.de 27.12.2015; Strittiges Anti-Terror-Gesetz, SZ 28.12.2015, 7; Beuth, Eine Hintertür für uns, aber bitte nicht für China, www.zeit.de 03.03.2015).

Technik-Nachrichten

Abgebildete Augenpaare disziplinieren Menschen

Ein Forschungsteam von PsychologInnen um Melissa Bateson und Daniel Nettle von der Universität Newcastle hat gemäß dem Fachjournal PeerJ (online) herausgefunden, dass bereits das Bild eines Augenpaares einen erzieherischen Effekt auf das Verhalten von Menschen hat: Da diese Darstellung daran erinnert, dass man beobachtet werden könnte, wird so die Wahrscheinlichkeit eines Normverstoßes reduziert.

Die ForscherInnen hängten an Fahrräder nahe ihrer Universität Karten mit einer Warnung vor Dieben und forderten dazu auf, ein sicheres Schloss zu verwenden. Sie interessierten sich nun dafür, wohin die mit dieser Nachricht traktierten Menschen die Postkarte am Rad „entsorgten", wenn sie losfahren wollten. War auf dem Flyer zusätzlich zur Botschaft ein Augenpaar zu sehen, dann sank die Wahrscheinlichkeit, dass die FahrradbesitzerInnen den Zettel einfach auf den Boden warfen. Lediglich 4,7% der Personen warfen das Papier unter diesen Bedingungen achtlos weg. Waren dagegen keine Augen auf dem Flyer, waren es 15,6% der von dem Versuch Betroffenen, die das Papier zwischen die Räder am Stellplatz zurückließen. Ähnliche Ergebnisse sind aus vergleichbaren Studien bekannt: Sind Augenpaare gut sichtbar an der Wand angebracht, hat dies den gleichen Effekt. In einem Versuch steigerten die Bilder die Ehrlichkeit von ProbandInnen, wenn diese ohne Kontrolle Geld für Kaffee in eine Kasse werfen sollten.

Nettle: „Es ist Menschen eben sehr wichtig, was andere von ihnen denken und wir verhalten uns anständiger, wenn wir uns beobachtet fühlen." Wer sich beobachtet fühlt, verhält sich mit höherer Wahrscheinlichkeit regelkonform. Die Gegenwart anderer übt einen disziplinierenden Einfluss auf Menschen aus. Manche Dinge macht man nur, wenn man sich unbeobachtet fühlt. Die PsychologInnen regen an, zum Beispiel Fast-Food-Verpackungen mit Augenpaaren zu bedrucken. Gut möglich, dass Städte so sauberer werden (Herrmann, Du wirst beobachtet, SZ 02.12.2015, 16 = www.sueddeutsche.de 01.12.2015).

Gesellschaftsanalyse per Mobilfunk-Auswertung

In vielen afrikanischen Staaten existieren keine zuverlässigen Daten über die Entwicklung von Bevölkerung und Wirtschaft. Durch Analyse des Mobilfunkverkehrs wollen WissenschaftlerInnen Erkenntnisse von Gesellschaften erlangen und ein sozio-demografisches Profil ganzer Nationen nachzeichnen. Informatiker um Joshua Blumenstock von der University of Washington in Seattle berichten im Fachjournal Science (Bd. 350, S. 1073, 2015), dass sie auf diese Weise die Verteilung von Wohlstand im afrikanischen Staat Ruanda abbilden können. Die Forschenden werteten die Daten von mehreren Milliarden Mobilfunk-Interaktionen in Ruanda aus und erstellten für einzelne Personen Bewegungsprofile, analysierten deren soziale Netzwerke und extrahierten außerdem Daten zum finanziellem Verhalten. So gelang es ihnen, ein exaktes Bild zu erstellen, wo in Ruanda Wohlstand oder Armut konzentriert sind. In vielen Entwicklungsländern existieren nur sehr ungenaue nationale Statistiken, etwa über die Verteilung von Einkommen, über die Industrieproduktion oder die geografische Konzentration von Armut. Häufig wichen die offiziellen Zahlen um mehr als 50 Prozent von den tatsächlichen Gegebenheiten ab. Weil aber auf Basis dieser Informationen politische Entscheidungen gefällt werden, ist das ein Problem (Reich oder arm? www.sueddeutsche.de 26.11.2015 = SZ 27.11.2015, 16).

Rechtsprechung

EGMR

Arbeitgeber darf private Arbeitnehmer-E-Mails überwachen

Der Europäische Gerichtshof für Menschenrechte (EGMR) hat in einem Urteil vom 12.01.2016 entschieden, dass die Überwachung der Internetnutzung eines Arbeitnehmers durch dessen Arbeitgeber keinen Verstoß gegen Artikel 8 der Europäischen Menschenrechtskonvention (Recht auf Achtung des Privat- und Familienlebens) darstellt, wenn die E-Mail-Nutzung auf dienstliche Zwecke beschränkt ist (Barbulescu/Rumänien, Beschwerdenr. 61496/08).

Der Beschwerdeführer, ein Ingenieur, hatte geltend gemacht, sein Recht auf vertrauliche Kommunikation sei verletzt worden, als die Chats für seine Kündigung verwendet wurden. Er war von seinem Arbeitgeber darüber in Kenntnis gesetzt worden, dass ein auf Anweisung seines Arbeitgebers eingerichtetes Yahoo-Messenger-Konto überwacht worden war und dass die Aufzeichnun-

gen eine private Nutzung auswiesen. Der Beschwerdeführer bestritt dies. Darauf hin wurden ihm die Protokolle seiner Kommunikation inklusive Nachrichten vorgelegt, die er mit seinem Bruder und seiner Verlobten über sein Gesundheits- und Geschlechtsleben ausgetauscht hatte. In der Folge wurde dem Beschwerdeführer gekündigt.

Nach dem EGMR-Urteil haben die heimischen Gerichte dem Antragsteller die Möglichkeit gegeben, seine Argumente zu einer Verletzung von Art. 8 EMRK vorzubringen. Außerdem hätten diese die Interessen des Beschwerdeführers in einen fairen Ausgleich mit denen des Arbeitgebers gebracht, unter anderem hätten sie in ihren Entscheidungen keine Einzelheiten über die E-Mail-Kommunikation genannt. Es sei vom Arbeitgeber nicht unbillig, die Arbeitsleistung des Arbeitnehmers während der Arbeitszeit überprüfen zu wollen (Didier, EGMR: Arbeitgeber darf private Arbeitnehmer-E-Mails überwachen, www.der-betrieb.de 21.01.2016; Gesellensetter, SZ 22.01.2016, 21).

BGH

Löschanspruch gegen Exfreund bei Bildern aus Intimsphäre

Der Bundesgerichtshof (BGH) bestätigte mit Urteil vom 13.10.2015 das Urteil des Oberlandesgerichts (OLG) Koblenz vom 20.04.2014, das einen Fotografen verpflichtete, Intimfotos seiner Freundin auf deren Aufforderung hin zu löschen (VI ZR 271/14). Die klagende frühere Freundin hatte mit dem Beklagten eine außereheliche intime Liebesbeziehung, in der einvernehmlich zahlreiche Bild- und Filmaufnahmen mit der Frau unbekleidet und bekleidet sowie vor, während und nach dem Geschlechtsverkehr entstanden, die der Beklagte speicherte. Schon in der Vorinstanz verpflichtete sich der Fotograf, die Bilder ohne die Einwilligung der Frau keinen Dritten zugänglich zu machen. Die Frau forderte ihn darüber hinausgehend dazu auf, sämtliche Bilder einschließlich Filme zu löschen bzw. Kopien zu vernichten.

Dieser Klage entsprach das Landgericht (LG) Koblenz in Bezug auf Nackt- und Intimbilder, nicht jedoch bezüglich der weniger verfänglichen Bilder. Dagegen legten beide Seiten Berufung ein, die jeweils vom OLG Koblenz zurückgewiesen wurde (vgl. DANA 1/2015, 49 f.). Der BGH bestätigte nun das OLG-Urteil. Den Löschanspruch begründete der BGH nicht mit dem Bundesdatenschutzgesetz (BDSG), da die Aufnahmen nicht zur Veröffentlichung bestimmt und ausschließlich zu persönlichen bzw. privaten Zwecken gefertigt worden sind (§§ 1 Abs. 2 Nr. 3, 27 BDSG). Das Gericht stützte den Anspruch auch nicht auf § 37 Kunsturhebergesetz (KUG), da die Bilder nicht widerrechtlich hergestellt wurden.

Als Rechtsgrund für den Löschanspruch erkannte der BGH vielmehr das aus dem allgemeinen Persönlichkeitsrecht abgeleitete und in den §§ 22 ff. KUG geschützte Recht am eigenen Bild an. Daraus ergibt sich „kein allgemeines oder gar umfassendes Verfügungsrecht über die Darstellung der eigenen Person“, wohl „aber Einfluss- und Entscheidungsmöglichkeiten, soweit es um die Anfertigung und Verwendung von Bildaufzeichnungen seiner Person durch andere geht. Das Schutzbedürfnis ergibt sich vor allem aus der Möglichkeit, das auf eine bestimmte Situation bezogene Erscheinungsbild eines Menschen davon zu lösen und das Abbild jederzeit unter für den Betroffenen nicht überschaubaren und/oder nicht beherrschbaren Voraussetzungen vor Dritten zu reproduzieren. Je leichter dies ist, desto größer kann das Schutzbedürfnis sein. So sind mit dem Fortschritt der Aufnahmetechniken wachsende Möglichkeiten der Gefährdung von Persönlichkeitsrechten verbunden“.

Der BGH stellte klar, dass die §§ 22 ff. KUG einen weitergehenden Bildnisschutz nicht ausschließen: „Danach kann unter besonderen Umständen schon das Innehaben der Verfügungsmacht über Bildaufnahmen durch einen Dritten gegen den Willen des Abgebildeten, sei es durch Behalten und Betrachten, dessen Persönlichkeitsrechte verletzen.“ Dies gilt vor allem, wenn die Privat- und Intimsphäre des Einzelnen und Aspekte des Geschlechtslebens tangiert sind: „Fehlte es hier an einem Schutz vor Kenntniserlangung anderer, wäre die sexuelle Entfaltung erheblich beeinträchtigt, obwohl es sich um grundrechtlich geschützte Verhaltensweisen handelt.“ Das Grundgesetz gewährt dem Einzelnen im Kernbereich höchstpersönlicher, privater Lebensgestaltung einen unantastbaren Bereich zur Entfaltung der Persönlichkeit, der wegen seiner besonderen Nähe zur Menschenwürde absolut geschützt und einer Einschränkung durch Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes nicht zugänglich ist“.

Die intimen Aufnahmen waren, so der BGH, diesem Kernbereich zuzuordnen: „Wer nämlich – wie hier – Bildaufnahmen und Fotografien, die einen anderen darstellen, besitzt, erlangt allein durch diesen Besitz eine gewisse Herrschafts- und Manipulationsmacht über den Abgebildeten, selbst wenn eine Verbreitung und Weitergabe an Dritte nicht beabsichtigt oder untersagt ist. Diese Macht ist umso größer, als Aufnahmen eine vollständige Entblößung des gänzlich Privaten, der grundsätzlich absolut geschützten Intimsphäre des Einzelnen, insbesondere im Zusammenhang mit gelebter Sexualität, zeigen. Diese Entblößung wird vom Abgebildeten regelmäßig als peinlich und beschämend empfunden, wenn sich der Situationszusammenhang wie hier durch die Beendigung der Beziehung geändert hat.

Der Umstand, dass sich die Klägerin dem Beklagten geöffnet hat, kann zwar zu einer Abwägungsentscheidung führen. „Diese Einwilligung war aber begrenzt auf die Dauer ihrer Beziehung zu dem Beklagten.“ Der Beklagte konnte als Fotograf auch nicht seine Berufsfreiheit wirksam machen, weil diese nicht berührt war. „Das ideelle Interesse des Beklagten, die Bilder zur Pflege der Erinnerung an die gemeinsame Beziehung behalten zu dürfen, kann eine schutzwürdige Rechtsposition schon deshalb nicht begründen, weil ihm der Gewahrsam an den Bildern von vornherein nur für die Dauer der Beziehung gestattet war. Aus entsprechenden Gründen ist dem Beklagten auch die Berufung auf Art. 14 GG oder die Kunstfreiheit (Art. 5 Abs. 3 GG) versagt“ (http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&Sort=12288&nr=73173&pos=24&anz=585).

BGH

Werbung in Kunden-E-Mail nach Widerspruch unzulässig

Der Bundesgerichtshof (BGH) hat mit Urteil vom 15.12.2014 entschieden, dass gegen den erklärten Willen eines Verbrauchers übersandte E-Mails mit werblichem Inhalt eine Verletzung des allgemeinen Persönlichkeitsrechts darstellen (VI ZR 134/15). Der Kläger hatte sich am 10.12.2013 mit der Bitte um Bestätigung einer von ihm ausgesprochenen Kündigung per E-Mail an seine Sparkassenversicherung, die Beklagte, gewandt. Diese bestätigte unter dem Betreff „Automatische Antwort auf Ihre Mail (…)“ den Eingang der E-Mail des Klägers:

„Sehr geehrte Damen und Herren, vielen Dank für Ihre Nachricht. Wir bestätigen Ihnen hiermit den Eingang Ihres Mails. Sie erhalten baldmöglichst eine Antwort. Mit freundlichen Grüßen, Ihre S. Versicherung.

Übrigens: Unwetterwarnungen per SMS kostenlos auf Ihr Handy. Ein exklusiver Service nur für S. Kunden. Infos und Anmeldung unter (…)

*Neu für iPhone Nutzer: Die App S. Haus & Wetter, inkl. Push Benachrichtigungen für Unwetter und vielen weiteren nützlichen Features rund um Wetter und Wohnen: (…) ***Diese E-Mail wird automatisch vom System generiert. Bitte antworten Sie nicht darauf.***“*

Der Kläger wandte sich daraufhin am 11.12.2013 erneut per E-Mail an den Datenschutzbeauftragten der Beklagten und rügte, die automatisierte Antwort enthalte Werbung, mit der er nicht einverstanden sei. Auch auf diese E-Mail sowie auf eine weitere mit einer Sachstandsanfrage vom 19.12.2013 erhielt der Kläger eine automatisierte Empfangsbestätigung mit dem obigen Inhalt.

Der Kläger verlangte von der Beklagten, es zu unterlassen, zum Zwecke der Werbung mit ihm, ohne sein Einverständnis per E-Mail Kontakt aufzunehmen oder aufnehmen zu lassen. Das Amtsgericht (AG) Stuttgart-Bad Cannstatt hatte mit Urteil vom 25.04.2014 einer entsprechenden Klage stattgegeben (10 C 225/14). Auf die Berufung der Beklagten hat das Landgericht (LG) Stuttgart das Urteil des AG am 04.02.2015 aufgehoben und die Klage abgewiesen (4 S 165/14). Die zugelassene Revision führte zur Aufhebung des Berufungsurteils des LG und zur Wiederherstellung des amtsgerichtlichen Urteils, weil die Übersendung der Bestätigungsmails mit Werbezusatz vom 19.12.2013 den Kläger in seinem allgemeinen Persönlichkeitsrecht verletzt hat, nachdem er zuvor sich ausdrücklich gegen derartige Zusendungen zur Wehr gesetzt hatte. Der Senatsvorsitzende Gregor Galke erklärte, jeder habe das Recht, „im privaten Bereich in Ruhe gelassen zu werden“. Der BGH hatte schon 1988 geklärt, dass „Kleine-Werbung-Aufkleber“ auf dem Briefkasten bei Reklamesendungen beachtet werden müssten. Diese Linie wurde bei Telefonwerbung ausgeweitet. Werbung ist hier nur nach erklärtem Einverständnis zulässig. Dies gilt nach dem Gesetz gegen unlauteren Wettbewerb auch für elektronische Post. Im aktuellen Fall hat der BGH offengelassen, ob bereits die erste E-Mail rechtswidrig war. Bei der zweiten und dritten Mail hatte der Kläger jedenfalls ausdrücklich seinen Widerspruch erklärt. Das LG Stuttgart hatte die Belästigung zuvor als unerheblich eingestuft, weil es sich nicht um „klassische“ Werbe-E-Mail gehandelt habe, sondern um einen Kontakt im laufenden Kundenverhältnis.

Praktisch oft schwer zu beantworten ist die Frage, wann eine VerbraucherIn ihre Einwilligung erteilt hat. Online-Einkäufe u. Ä. sind oft mit der Aufforderung verbunden, elektronischer Reklame zuzustimmen. Heiko Dünkel vom Verbraucherzentrale Bundesverband (vzbv) wies darauf hin, dass Verbraucherzentralen Unternehmen wegen ungewollter E-Mail-Werbung abmahnen dürfen, weshalb dort entsprechende Beschwerden eingereicht werden können (BGH, PE v. 16.12.2015, Nr. 204/15, Bundesgerichtshof zur Zulässigkeit sogenannter „No-Reply“ Bestätigungsmails mit Werbezusätzen; Janisch, Nerven verboten, SZ 17.12.2015, 19).

BGH

Facebook-Freundefinder war unzulässig

Der unter anderem für das Wettbewerbsrecht zuständige 1. Zivilsenat des Bundesgerichtshofs (BGH) entschied mit Urteil vom 14.01.2016, dass die mithilfe der Facebook-Funktion „Freunde finden“ versendeten Einladungs-E-Mails an Personen, die nicht als „Facebook“-Mitglieder registriert sind, eine wettbewerbsrechtlich unzulässige belästigende Werbung darstellen (I ZR 65/14). Zudem stellte das Gericht fest, dass Facebook im Rahmen des im November 2010 zur Verfügung gestellten Registrierungsvorgangs für die Funktion „Freunde finden“ die Nutzenden über Art und Umfang der Nutzung von importierten Kontaktdaten irregeführt hat.

Geklagt hatte der Bundesverband der Verbraucherzentralen und Verbraucherverbände in Deutschland (vzbv). Der vzbv wendete sich mit einem Unterlassungsanspruch dagegen, dass Facebook bei der von ihr bereit gestellten Funktion „Freunde finden“ die Nutzenden dazu veranlasste, ihre E-Mail-Adressdateien in den Datenbestand von Facebook zu importieren und Einladungs-E-Mails an bisher nicht als Nutzende der Plattform registrierte Personen zu senden. Dies sei eine die EmpfängerInnen belästigende Werbung im Sinne von § 7 Abs. 1 und 2 Nr. 3 des Gesetzes gegen unlauteren Wettbewerb (UWG). Der vzbv beklagte ferner, Facebook täusche die Nutzenden

im Rahmen des Registrierungsvorgangs in unzulässiger Weise darüber, in welchem Umfang die von den Nutzenden importierten E-Mail-Adressdateien von Facebook genutzt würden. Das Landgericht hat der Klage stattgegeben. Die Berufung Facebooks war ohne Erfolg geblieben.

Facebook-Anwalt Thomas von Plehwe hatte bei der Verhandlung mit der altruistisch klingenden „Philosophie“ des Unternehmens argumentiert. Bei der Freunde-finden-Mail „handelt es sich um den Wunsch des Nutzers, sein Netzwerk aufzubauen.“ Verbraucher-Anwalt Peter Wassermann hatte erwidert: „Es geht maßgeblich darum, aus geschäftlichen Interessen neue Mitglieder für das Netzwerk zu gewinnen.“ Der BGH wies die Revision von Facebook zurück und stellte fest, dass Einladungs-E-Mails von Facebook an Empfänger, die in den Erhalt der E-Mails nicht ausdrücklich eingewilligt haben, eine unzumutbare Belästigung im Sinne des § 7 Abs. 2 Nr. 3 UWG sind. Die Einladungs-E-Mails sind Facebook-Werbung, auch wenn ihre Versendung durch die registrierten Nutzenden ausgelöst wird, weil es sich um eine von der Beklagten zur Verfügung gestellte Funktion handelt, mit der Dritte auf das Angebot von Facebook aufmerksam gemacht werden sollen. Die Einladungs-E-Mails würden von den EmpfängerInnen nicht als private Mitteilung der Facebook-Nutzers, sondern als Werbung der Beklagten verstanden.

Durch seine Angaben hatte Facebook im November 2010 bei der Registrierung für die Facebook-Funktion die sich registrierenden Nutzenden unter Verstoß gegen § 5 UWG über Art und Umfang der Nutzung der E-Mail-Kontaktdaten getäuscht. Der im ersten Schritt des Registrierungsvorgangs eingeblendete Hinweis „Sind deine Freunde schon bei Facebook?“ klärte nicht darüber auf, dass die vom Nutzer importierten E-Mail-Kontaktdaten ausgewertet werden und eine Versendung der Einladungs-E-Mails auch an Personen erfolgt, die noch nicht bei Facebook registriert sind. Die unter dem elektronischen Verweis „Dein Passwort wird von Facebook nicht gespeichert“ hinterlegten weitergehenden Informationen konnten die Irreführung nicht ausräumen, weil ihre Kenntnisnahme durch den Nutzenden nicht sichergestellt war.

Facebook hat seine Bedingungen inzwischen geändert, neu registrierte Nutzende haben nun mehr Einfluss darauf, an wen Einladungen verschickt werden. Zwar dürften Einladungsmails an Nichtnutzende nach wie vor rechtlich äußerst problematisch sein, jedenfalls dann, wenn sie von Facebook vorformuliert sind. Was aber beispielsweise für das Hochladen der Adressdateien von NeukundInnen gilt, werden wohl erst weitere Prozesse klären. Im Karlsruher Fall war die Verbraucherinformationen zur Nutzung der abgesaugten Adressen ziemlich undurchsichtig. Inzwischen ist sie nach Einschätzung des vzbv transparenter, aber immer noch nicht klar genug.

Die juristische Auseinandersetzung um die sozialen Netzwerke stehen erst am Anfang. In einem derzeit beim Landgericht Berlin anhängigen Verfahren spielt ebenfalls die kommerzielle Natur des Netzwerks eine Rolle. Die Verbraucherzentrale hat Facebook wegen der Werbeaussage „Facebook ist und bleibt kostenlos“ verklagt, weil die VerbraucherInnen für ihren Facebook-Account zwar nicht in Euro, aber mit ihren Daten bezahlten. In dem Prozess wird es zudem darum gehen, ob Voreinstellungen wie etwa der aktivierte Ortungsdienst auf einem Nutzeraccount zulässig sind. Außerdem geht es um eine Klausel, welche die Datenweitergabe an die USA zulässt. Bei Facebook&Co läuft also ein Dauerkonflikt ab: Die Verbraucherzentralen klagen, die Gerichte verurteilen, die Unternehmen bessern halbherzig nach. Woraufhin die Verbraucherzentralen wieder klagen... (Bundesgerichtshof zur Facebook-Funktion „Freunde finden“, PE Nr. 7/2016 v. 14.01.2016; Janisch, Geschäft mit Freunden, SZ 15.01.2016, 10).

OVG Berlin

Bundestag muss LobbyistInnen offenlegen

Das Oberverwaltungsgericht (OVG) Berlin hat mit Beschluss vom 20.11.2015 in einem vorläufigen Rechtsschutzverfahren entschieden, dass der Deutsche Bundestag JournalistInnen Auskunft darüber geben muss, welche LobbyistInnen sich mit Hausausweis im Parlament bewegen (Az. OVG 6 S 45.15), und bestätigte damit eine Entscheidung der Vorinstanz.

Der Bundestag erteilt Hausausweise, die zum Zugang des Parlamentes berechtigen, an InteressenvertreterInnen. Ein Teil der Verbände ist in eine offen einsehbare Liste eingetragen. Doch erhalten auch nicht registrierte LobbyistInnen den Ausweis, wenn sie mit einem vom Parlamentarischen Geschäftsführer einer Fraktion gezeichneten Antrag nachweisen, dass sie die Bundestagsgebäude im Interesse des Parlaments häufig aufsuchen müssen. Die Zeitung Tagesspiegel hatte dem Bundestag hierzu die Frage gestellt, an welche Verbände, Organisationen und Unternehmen in der laufenden Legislaturperiode auf Grund der Befürwortung von Fraktionen Hausausweise erteilt worden sind, um wie viele es sich handelt und welche Fraktion dies jeweils befürwortet hat. Linke, Grüne und SPD-Fraktion haben ihre Lobby-Liste freiwillig offengelegt, die CDU/CSU-Fraktion nicht. Nach einer Weigerung auch des Parlaments hatte die Zeitung den Eilantrag gestellt.

Das OVG begründete seinen Beschluss damit, dass der Auskunftsanspruch Interessen des freien Bundestagsmandates nicht entgegen stehe. Die in Art. 38 Abs. 1 GG geschützte Freiheit des Mandats erfasse zwar auch das Informationsbeschaffungsverhalten der Bundestagsabgeordneten als Teil des parlamentarischen Willensbildungsprozesses. Die begehrten Auskünfte ließen aber keine Rückschlüsse darauf zu, ob bzw. wie häufig einzelne Abgeordnete mit InteressenvertreterInnen, die InhaberInnen von Hausausweisen sind, zu Gesprächen in den Räumen des Bundestages zusammenkommen. Dies gelte auch für die Parlamentarischen Geschäftsführer, die lediglich stellvertretend für ihre Fraktion die Anträge auf Erteilung von Hausausweisen befürworten. Daher sei nicht ersichtlich, dass die Auskunftserteilung das Kommunikationsverhalten einzelner Abgeordneter beeinträchtigen könnte. Eine Verletzung des Rechts auf informationelle Selbstbestimmung der InteressenvertreterInnen verneinte der Senat ebenfalls. Der

Beschluss des OVG ist unanfechtbar (Bundestag muss Lobbyisten-Liste offenlegen, www.lto.de 20.11.2015).

OLG München

Schumachers Privatsphäre geht vor

Das Oberlandesgericht (OLG) München wies mit Urteil vom 19.01.2016 eine Berufung von Medienunternehmen gegen entsprechende Urteile weitestgehend zurück, die Unterlassungsklagen gegen vier Zeitschriften stattgegeben hatten, die eine Pressemitteilung von Michael Schumachers Sprecherin zu dessen Gesundheitszustand ausschmückten. Die Medien seien zu weit in die Privatsphäre des ehemaligen Formel-1-Weltmeisters eingedrungen. Eine Revision gegen die in vier Einzelfällen gesprochenen Urteile schloss der Senat aus. Das OLG stellte in der Verhandlung klar, dass ein Berichterstattungsinteresse über den Gesundheitszustand einer der berühmtesten Personen Deutschlands durchaus bestehe. Andererseits habe auch eine Person des öffentlichen Lebens ein Recht auf Privatsphäre. Der ehemalige Formel-1-Weltmeister war am 29.12.2013 beim Skifahren schwer verunglückt. Der mittlerweile 47-Jährige hatte sich bei seinem Sturz ein schweres Schädel-Hirn-Trauma zugezogen und tagelang um sein Leben gekämpft (OLG: Medien drangen zu stark in Schumachers Privatsphäre ein, www.focus.de 20.01.2016).

VG Neustadt

Keine Bearbeitungsfristen bei Datenschutzeingaben

Das Verwaltungsgericht (VG) Neustadt hat mit Beschluss vom 22.12.2015 entschieden, dass der Landesbeauftragte für den Datenschutz und die Informationsfreiheit in Baden-Württemberg (LDI BW) im Rahmen seiner Beratungs- und Informationstätigkeit gegenüber den Bürgerinnen und Bürgern in Fragen des Datenschutzes und der Datensicherheit nicht an gesetzliche Fristen gebunden ist. Es komme auf die konkreten Umstände des Einzelfalles an, innerhalb welcher Frist der LDI einen Petenten zu bescheiden hat.

Der Beschluss erging im Rahmen eines Prozesshilfeverfahrens. Der Kläger und Antragsteller hatte am 07.10.2014 eine datenschutzrechtliche Überprüfung der Kreissparkasse Südwestpfalz gefordert, weil die Diskretion bei Kundengesprächen nicht beachtet werde, Mitarbeitende von Umstand des Bezugs von Arbeitslosengeld in Kenntnis seien und Kontoauszüge nicht datenschutzgerecht versendet würden. Der LDI BW antwortete dem Kläger erstmals am 16.10.2014 überschlägig. Am 09.03.2015 berichtete der LDI BW nach Auswertung des Antwortschreibens der Sparkasse. Am 19.06. forderte der Kläger einen schriftlichen Bescheid und die Benennung einer übergeordneten Beschwerdestelle. Eine abschließende Bewertung wurde am 13.08. verfasst, aber erst am 11.09.2015 versandt. Bereits zuvor, am 04.09.2015 erhob der Petent Untätigkeitsklage. Der Prozesshilfeantrag wurde abgelehnt, weil die Klage keine Aussicht auf Erfolg habe.

„In der Rechtsprechung ist geklärt, dass auf Petitionen und Dienstaufsichtsbeschwerden ergehende Bescheide keine Verwaltungsakte sind. ... Ein Petitionsbescheid regelt nichts mit unmittelbarer rechtlicher Außenwirkung, sondern stellt nur die tatsächliche Erfüllung der Verpflichtung aus Art 17 Grundgesetz – GG – bzw. Art. 11 LV (Landesverfassung Baden-Württemberg) dar. … Art. 11 LV gewährt aber kein Recht auf Erledigung der Petition im Sinne des Petenten und auch keinen Anspruch darauf, Art und Umfang der sachlichen Prüfung der Petition einer gerichtlichen Kontrolle zu unterziehen. ... Auch Art. 19 Abs. 4 Satz 1 GG gebietet nicht die Zulassung von Anfechtungsklagen gegen ablehnende Petitionsbescheide oder Verpflichtungsklagen auf Erlass von positiven Petitionsbescheiden.“ Deshalb sei die Untätigkeitsklage nicht statthaft.

Auch als Leistungsklage habe das Anliegen des Klägers keine Aussicht auf Erfolg: „Der Kläger hat zwar einen mit der allgemeinen Leistungsklage durchsetzbaren Anspruch auf Erteilung eines informatorischen Bescheides über die Art und Weise der Erledigung seiner Petition. … Wie oben bereits ausgeführt, gewährt Art. 11 LV aber kein Recht auf Erledigung der Petition im Sinne des Petenten und auch keinen Anspruch darauf, Art und Umfang der sachlichen Prüfung der Petition einer gerichtlichen Kontrolle zu unterziehen. Denn dann erhielte das Petitionsrecht die Funktion einer Popularklage. Der Beklagte hat im Übrigen den Anspruch des Klägers auf Entgegennahme seiner Petition, auf sachliche Befassung mit seiner Eingabe und auf Bescheidung der Eingabe, aus der ersichtlich wird, dass und mit welchem Ergebnis sie behandelt wurde, spätestens mit am 11. September 2015 übersandten Schreiben erfüllt. …

Der LDI ist im Rahmen seiner Beratungs- und Informationstätigkeit gegenüber den Bürgerinnen und Bürgern in Fragen des Datenschutzes und der Datensicherheit nicht an gesetzliche Fristen gebunden. Es kommt daher auf die konkreten Umstände des Einzelfalles an, innerhalb welcher Frist der LDI einen Petenten zu bescheiden hat. … Ausgehend von diesem Sachverhalt kann nach Auffassung der Kammer keine Rede davon sein, dass der LDI den Kläger nicht zeitnah beschieden hat. … Selbst wenn man sich für die Beantwortung der Frage, innerhalb welchen Zeitraums ein Petent mit der Bescheidung seiner Eingabe durch den LDI rechnen darf, an der Dreimonatsfrist des § 75 VwGO orientieren würde, lagen hier zureichende Gründe im Sinne des § 75 VwGO ... vor, das Begehren des Klägers abschließend nicht vorher zu bescheiden“ (Landesdatenschutzbehörde muss Bürgeranfragen nicht innerhalb bestimmter Fristen bearbeiten, www.datenschutz.eu Januar 2016).

LG Berlin

Eltern erhalten Zugang zu Facebook-Konto von verstorbener Tochter

Gemäß einem Urteil des Landgerichts (LG) Berlin vom 17.12.2015 haben Eltern einer minderjährig Verstorbenen Anspruch gegen den Betreiber eines sozialen Netzwerks auf Herausgabe der Zugangsdaten zu dem Benutzerkonto ihrer Tochter (20 O 172/15). Die Tochter der Klägerin war mit 15 Jahren unter un-

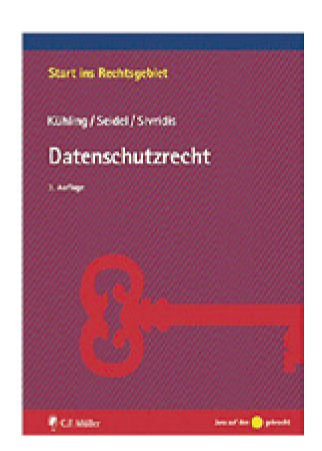
geklärten Umständen durch eine in einen Bahnhof einlaufende U-Bahn tödlich verletzt worden. Die Klägerin erhoffte, über den Facebook-Account ihrer Tochter und die dort ausgetauschten Nachrichten und Posts mehr über den Tod ihrer Tochter zu erfahren und zu klären, ob es sich um einen Selbstmord gehandelt haben könnte. Dies war auch deshalb von Bedeutung, da der Fahrer der U-Bahn, die die Verstorbene erfasst hatte, gegen die Erben ein Schmerzensgeld und Schadenersatz wegen Verdienstausfalls geltend machte. Facebook Ireland Limited (im Folgenden: Facebook) verweigerte der Klägerin die Zugangsdaten zu dem in einen Gedenkzustand versetzten Account, so dass diese Klage erhob.

Das der Klage stattgebende LG verpflichtete Facebook, den Eltern der Verstorbenen als deren Erben Zugang zu dem Benutzerkonto und dessen Kommunikationsinhalten zu gewähren. Der Vertrag zur Nutzung der Facebook-Dienste, den die Tochter abgeschlossen hatte, sei wie jeder andere schuldrechtliche Vertrag auf die Erben übergegangen. Eine unterschiedliche Behandlung des digitalen und des „analogen“ Vermögens des Erblassers sei nicht gerechtfertigt. Eine Ungleichbehandlung würde dazu führen, dass persönliche Briefe und Tagebücher unabhängig von ihrem Inhalt vererblich wären, E-Mails oder private Facebook-Nachrichten hingegen nicht.

Dem stünden keine schutzwürdige Interessen von Facebook entgegen. Der Nutzungsvertrag werde regelmäßig ohne nähere Prüfung des Nutzers abgeschlossen. Die Identität kontrolliere Facebook nur in Ausnahmefällen. Ebenso stehe das postmortale Persönlichkeitsrecht der Verstorbenen einer Zugangsgewährung nicht entgegen. Denn die Erziehungsberechtigten seien für den Schutz des Persönlichkeitsrechtes ihrer minderjährigen Kinder zuständig. Dies gelte nicht nur zu deren Lebzeiten. Jedenfalls dann, wenn besondere Umstände wie hier die ungeklärte Todesursache der Tochter vorlägen, seien die Eltern als Erben berechtigt, sich Kenntnis darüber zu verschaffen, was ihre Tochter im Internet geäußert hat.

Die Gedenkzustands-Richtlinie, wie sie Facebook vor 2014 verwandt hatte, sei unwirksam. Es stelle eine unangemessene Benachteiligung der Nutzenden bzw. deren Erben dar, wenn eine beliebige Person der Facebook-Freundesliste veranlassen könnte, dass das Profil des Nutzers in den Gedenkzustand versetzt wird, und wenn dies auch von den Erben nicht rückgängig gemacht werden kann. Auch das Datenschutzrecht stehe dem Anspruch auf Zugangsgewährung nicht entgegen. Vertrauliche Briefe, die ein Dritter verschickt habe, könnten nach dem Tod des Empfängers von den Erben gelesen werden, ohne dass ein Eingriff in die Rechte dieser Dritten vorliege. Nichts Anderes gelte für digitale Daten. Facebook hat Berufung gegen das Urteil eingelegt (Landgericht Berlin: Eltern einer minderjährig Verstorbenen erben Facebook-Account ihrer Tochter, http://www.kostenlose-urteile.de 07.01.2016; Eltern erben Account, Facebook wehrt sich, SZ 02.02.2016, 10).

Buchbesprechungen



Kühling, Jürgen/Seidel, Christian/
Sivridis, Anastasios
Datenschutzrecht, 3. Aufl. 2015, 314 S.
ISBN 978-3-8114-9486-2

(tw) Als explizite Ausbildungsliteratur für JuristInnen im Bereich des Datenschutzrechts hat sich das Buch, das in erster Auflage 2008 erschien, etabliert. Es führt in die grundlegenden rechtlichen Fragestellungen des Datenschutzes in allgemein verständlicher Form ein. Anhand von 15 Fällen mit jeweiligen Lösungsskizzen wird die für Studierende wichtige Methode der stringenten Abarbeitung der relevanten Fragestellungen eingeübt. Die dabei verwendeten Fälle sind aktuell von Gerichten entschiedene Verfahren. Die Autoren folgen bei ihren Lösungen regelmäßig der gerichtlichen Entscheidung, weisen bei Abwägungsentscheidungen aber darauf hin, dass auch anders hätte entschieden werden können.

Die Darstellung ist insofern interessant, als sie nicht, wie üblich, mit dem Volkszählungsurteil und dem deutschen Bundesdatenschutzgesetz beginnt, sondern zunächst europarechtlich (Europarat, Unionsrecht) einsteigt, um dann aber ausführlich wichtige Fragestellungen des nationalen privaten wie öffentlichen Datenschutzrechts zu behandeln. Die aktuellen Fragen des Datenschutzes, bei denen das Internet und die internationale Datenverarbeitung eine wichtige Rolle spielen, stehen im Vordergrund. Nicht besonders vertieft werden – abgesehen vom Telekommunikations- und Telemedienrecht – bereichsspezifische Fragen. Im Fokus stehen auch nicht technische Fragestellungen, doch knüpft die Darstellung an der technischen Realität korrekt an. Redaktionsschluss war September 2015, Entwicklungen bis dahin sind berücksichtigt.

Das Buch ist übersichtlich gegliedert. Quellen zum Vertiefen werden nachvollziehbar wiedergegeben. Eine umfangreiche Gliederung und ein Stichwortverzeichnis erschließen auch

zielgerichtete Einzelausführungen. Das Lehrbuch ist also für JuristInnen, die einen Einstieg in das nicht gerade übersichtliche und einfache Datenschutzrecht suchen, sehr zu empfehlen.



Jacobs, Joachim
Vernetzte Gesellschaft. Vernetzte Bedrohungen
Berlin 2015, ISBN 978-3-945219-16-4, 350 S.

(tw) Der Umfang von Literatur zu Gefahren der Digitalisierung nimmt weiter zu. Dabei werden die unterschiedlichsten Schwerpunkte gesetzt. Das Taschenbuch von Joachim Jacobs erweitert das Spektrum um eine sehr journalistische Version: In seiner fulminanten, sehr assoziativen Zusammenstellung werden knapp 1.000 Pressemeldungen zur Digitalisierung verarbeitet und aneinandergereiht. Dabei wird vieles erwähnt, was mit Datenschutz, Datensicherheit, Big Data, Informationstechnikeinsatz hier und dort … zu tun hat, von der elektronischen Gesundheitskarte bis zu den Geschäftsmodellen im Internet oder im Gesundheitsbereich, vom E-Government bis zum Hacking, von Geheimdienstsabotage bis zur digitalen Freizeitgestaltung, von der Biometrie bis zum RFID, von Deutschland über die USA und die Welt wieder zurück nach Deutschland. Dabei werden die heute bestehenden technischen Möglichkeiten präsentiert, von der Datenpanne in der Sparkasse bis hin zum Einsatz sog. Künstlicher Intelligenz durch fremde Dienste, die daraus resultierenden Begehrlichkeiten, die Unfähigkeit damit sicher und verantwortungsvoll umzugehen auf der einen Seite und die Fähigkeit vieler Angreifer, diese Unfähigkeit zu nutzen.

Der Autor präsentiert Fakten, Fakten, Fakten, soweit diese sich aus journalistisch aufbereiteten Beiträgen oder eigenen Recherchen ergeben. Da aber die Breite des Stoffes zu groß ist, um alles in der Tiefe zu ergründen, präsentiert der Autor Zitate, Zitate, Zitate von – zweifellos durch die Bank – ausgewiesenen ExpertInnen auf ihrem jeweiligen Gebiet. Bei der Lektüre beschleicht einen immer mehr ein Unwohlsein bei allem, was mit Digitalem zu tun hat: Alles ist unsicher, gefährlich, zumindest problematisch, schwarz-weiß gezeichnet, aber fast ausschließlich schwarz. Insofern erfüllt das Buch eine Funktion: Verunsichern, evtl. auch aufrütteln. Es ermutigt zum Misstrauen.

Was das Buch nicht bietet und offensichtlich auch gar nicht bieten will, ist eine vertiefte Analyse, sei sie nun technisch, philosophisch, sozial, politisch, ökonomisch; abwägende Bewertungen und graduelle Einstufungen sind selten zu finden. Das Bewerten überlässt der Autor der geneigten LeserIn, die damit oft überfordert sein wird, auch weil die vielen erzählten Geschichten nur angerissen und nicht mit den Hintergründen erzählt werden können. Man könnte dem Buch deshalb Alarmismus vorwerfen, doch das würde voraussetzen, dass Bedrohungen für konkret benannte Werte dargestellt würden. Doch auch insofern lässt einen das Buch allein, so dass die erzählten Geschichten zwangsläufig an den eigenen unhinterfragten Werten gemessen werden. Vielleicht hat der Autor das gewollt; explizit gemacht hat er diese Intention jedoch nicht.

Das macht neugierig auf das letzte Kapitel, das mit „Schutzmöglichkeiten" überschrieben ist. Wer jedoch nun vermutet hätte, dass der Adressat des Buches die einzelne BürgerIn wäre, der wird enttäuscht. Angesprochen werden eher Unternehmens-, Behörden- und IT-Verantwortliche, denen sehr allgemein gehaltene Tipps für ein besseres Datenmanagement gegeben wird. Ob diese sich nach all der vorangegangenen Verunsicherung dadurch wieder aufbauen lassen, muss Spekulation bleiben.



Arndt/Fetzer/Scherer/Graulich,
Telekommunikationsgesetz, Kommentar,
2. Aufl. 2015, Erich Schmidt Verlag, Berlin, 2640 S., 284,00 EUR

(sh) Er kommt schon gewaltig daher, der „Berliner Kommentar" zum TKG, und bringt sich in Stellung gegen den Beck'schen TKG-Kommentar, welcher bei ähnlichem Format und Preis auf dem Gesetzesstand von 2012 verfügbar ist. Der auf dem Stand von Mai 2015 einschließlich des IT-Sicherheitsgesetzes beruhende Kommentar stammt auch in der 2. Auflage im Wesentlichen aus der Feder von auf Regulierungsfragen spezialisierten Wissenschaftlern, Angehörigen der Aufsichtsbehörden und Anwälten einer großen Frankfurter Rechtsanwaltskanzlei mit Schwerpunkt Wirtschaftsberatung. Als Vollkommentierung zum TKG ist das Werk von vorn herein mehr als eine Nummer zu groß für alle, die sich im Wesentlichen auf Datenschutzperspektive mit dem Telekommunikationsgesetz befassen und an der gebotenen ausführlichen Orientierung zu Regulierungs- und Ordnungsfragen keinen Bedarf haben. Aber wie steht es um die Beiträge zu den immer wieder datenschutz- und bürgerrechtlich entscheidenden Vorschriften im Telekommunikationsgesetz? Der dem Datenschutz gewidmete Abschnitt (§§ 91 – 107 TKG) wird anschaulich, klar strukturiert und mit Blick auf die gemeinschaftsrechtlichen Grundlagen behandelt, ohne dass die Kommentierung leidenschaftlich ausfällt oder für die Verbraucher bedeutende Rechtsprobleme zu lösen hätte. Das Schattendasein der Vorschriften zeigt sich auch daran,

dass der Kommentator so gut wie garnicht auf Rechtsprechung ein zu gehen hatte. Weniger zügig und knapp hingegen fällt das Werk an den Schnittstellen zu den öffentlichen Bedarfsträgern (§ 108 ff.) und zum grundrechtlichen Fernmeldegeheimnis (§ 88 ff.) aus. Dazu äußert sich ein Kommentator, dessen Personalie aufhorchen lässt: Auch in der 2. Auflage ist der frühere Richter am Bundesverwaltungsgericht Kurt Graulich dabei, den die Öffentlichkeit zuletzt als Sondergutachter zu bestimmten Aspekten der Beteiligung deutscher Stellen an der Überwachungstätigkeit der NSA kennengelernt hatte. Der Autor nutzt den ihm eingeräumten Platz, um gerade auch umstrittene Vorschriften wie § 113 TKG zu durchdringen und verfassungsrechtlich zu beleuchten. Seine Kommentierung fällt dabei gründlich, entlang der Verfassungsrechtsprechung, aber auch mit klarer Orientierung an den Zielen des Gesetzgebers aus. Der Verzicht auf eine obligate Kundendatenerhebung bei E-Mail-Accounts (§ 113 Abs. 1 S. 3 TKG) entlockt dem Autor nur wenige, distanzierte Zeilen. Wie hält es der Kommentar daher mit dem Schutz des Fernmeldegeheimnisses bei der erlaubten Nutzung betrieblicher E-Mail-Konten durch Arbeitnehmer? Auch bei dieser praktisch bedeutenden Frage wird das Werk leider wortkarg: Mit Bezugnahme auf eine Entscheidung des Landesarbeitsgerichts Berlin-Brandenburg (v. 16.02.2011 – 4 Sa 2132/10) belässt es der Autor bei der Wiedergabe der These, dass ein Arbeitgeber nicht Dienstanbieter i.S. § 88 Abs. 2 TKG sei. Auf eine ganze arbeitsrechtliche Bibliothek, die anderer Auffassung ist, nimmt der Autor keine Rücksicht. An dieser Stelle hätte der Leser aus der Datenschutzpraxis mehr erwartet, zumal die Anwendbarkeit des Fernmeldegeheimnisses auf die private Nutzung dienstlicher E-Mail-Anschlüsse unter Arbeitsrechtlern weiterhin herrschende Meinung sein dürfte. Kleines Trostpflaster: Der Kommentator der allgemeinen Begriffsbestimmungen (hier: § 3 Nr. 6 TKG) hält es – ebenso knapp begründet – entgegen seinem Kollegen mit der herrschenden Meinung.

Kaufen wird das Werk wohl, wer sich auf hohem Niveau über das ganze Telekommunikationsgesetz orientieren muß. Verbraucher- und Datenschützer sollten vor allem dann zu diesem Kommentar greifen, wenn sie die Position ihrer Gegenüber aus Behörden und Unternehmen verstehen wollen.

Cartoon




Freiheit